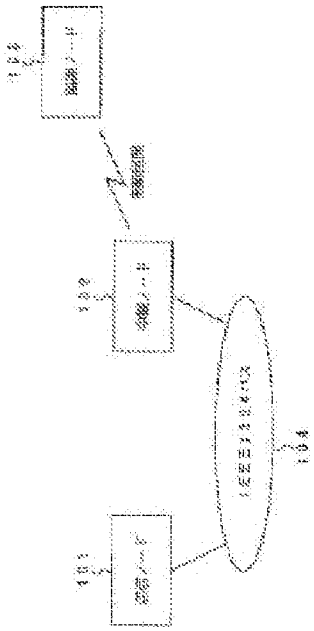
REPEATER AND COMMUNICATION EQUIPMENT

Publication number: JP2000174797 (A)
Publication date: 2000-06-23
Inventor(s): SAITO TAKESHI; TAKAHATA YOSHIAKI
Applicant(s): TOKYO SHIBAURA ELECTRIC CO
Classification:
- international: ***G11B20/10; G06F12/14; G06F21/24; H04H60/23; H04K1/00; H04L9/08; H04L9/32; H04L12/28; H04L12/46; H04L12/66; H04L29/06;*** *G11B20/00;* **G11B20/10; G06F12/14; G06F21/00; H04H1/00; H04K1/00; H04L9/08; H04L9/32; H04L12/28; H04L12/46; H04L12/66; H04L29/06;** G11B20/00; (IPC1-7): H04L12/46; G11B20/10; H04L9/32; H04L12/28; H04L12/66; H04L29/06
- European: H04L29/06S6A; H04H20/02; H04H60/23; H04K1/00; H04L9/08D2; H04L29/06S2D; H04L29/06S8
Application number: JP19990209836 19990723
Priority number(s): JP19990209836 19990723; JP19980292824 19980930

Also published as:
JP3583657 (B2)
US7218643 (B1)
US2007201511 (A1)

Abstract of **JP 2000174797 (A)**

PROBLEM TO BE SOLVED: To provide a repeater capable of a contents protection procedure between equipment not connected to the same network. SOLUTION: This repeater is connected to a first network 104 and a second network and is provided with a function for presenting the equipment 103 on the second network to the side of the first network 104 as the one on the present repeater 102, the function for transmitting a corresponding control command to the equipment 103 in the case of receiving the control command addressed to the equipment 103 from the equipment 101 on the first network 104,; the function for transmitting contents protection information to the equipment 103 without changing it in the case of receiving it addressed to the equipment 103 from the equipment 101 and the function for transmitting contents to the equipment 103 without changing them in the case of receiving the contents protected by a contents key obtained from the previous contents protection information from the equipment 101 to the equipment 103.



REPEATER AND COMMUNICATION EQUIPMENT

Description of corresponding document: **US 7218643 (B1)**

BACKGROUND OF THE INVENTION

[0001] 1. Field of the Invention

[0002] The present invention relates to a relay device for relaying data transfer between networks such as IEEE 1394 buses and radio networks, and a communication device for carrying out communications through a network such as IEEE 1394 bus and radio network.

[0003] 2. Description of the Background Art

[0004] In recent years, the so called "digitalization of home AV environment" is attracting much attentions as exemplified by the beginning of the digital broadcasting and the sales of digital AV instruments. Digital AV data have some excellent characteristics including the fact that various compression schemes are applicable, the fact that they can be processed as multimedia data, the fact that they are not degraded no matter how many times they are playbacked, etc., so that they are expected to have even wider use in future.

[0005] However, this digital AV technique has another aspect that "an illegal copy of contents can be made easily". Namely, for any digital contents, it is in principle possible to produce a copy with the same quality as the original, that will not degrade at all forever, by making "bit copy" so that the so called "illegal copy" problem arises.

[0006] Some techniques for preventing this "illegal copy" are currently discussed, including "1394CP Content Protection system Specification" that is discussed by the CPTWG (Copy Protection Technique Working Group). In this technique, for contents (such as MPEG data for example) to be transferred between nodes connected to the IEEE 1394 bus, the authentication between the transmitting and receiving nodes is carried out in advance so as to enable the sharing of an encryption key (contents key), and the contents are subsequently transferred by encrypting the contents such that the contents cannot be read by anyone except for those who have carried out the authentication procedure. In this way, a node that has not carried out the authentication procedure cannot ascertain the value of the contents key so that even if the transferred data (encrypted data) are obtained by such a node, the encrypted data cannot be decrypted by such a node. By making a rule that nodes that can participate in the authentication are only those nodes that are permitted by a prescribed authentication authority, it is possible to prevent an illegal node from acquiring the encryption key so that it is possible to prevent the illegal copy.

[0007] The IEEE 1394 bus is a network system having some very excellent characteristics including the fact that its speed is 100 Mbps at least, the fact that the network itself is equipped with an automatic configuration recognition function, the fact that it has a QOS transfer function, etc., so that it has been established as the de facto standard of a network for home digital AV use.

[0008] However, because of these characteristics, the IEEE 1394 also give rise to various constraints in the case of "connecting the IEEE 1394 with other networks". For example, in the case of connecting the IEEE 1394 bus with a radio network or a public network, it is impossible to directly extend the IEEE 1394 protocol to the radio network or the public network, because these networks are not as fast as over 100 Mbps in general and the automatic configuration recognition function of the IEEE 1394 cannot be directly extended to these networks so easily. For this reason, There are some propositions including a method in which a protocol conversion gateway is provided between the IEEE 1394 and the other network such as radio network or public network so as to interconnect them, and a method using the so called proxy server for providing services on one network as services on the other network.

[0009] In the case of attempting to apply these methods to the 1394 copy protection described above, currently the copy protection technique is defined only for the IEEE 1394 bus and currently there is no technique for extending this copy protection technique to the case of "connecting the IEEE 1394 with the other network".

SUMMARY OF THE INVENTION

[0010] It is therefore an object of the present invention to provide a relay device and a communication device capable of extending the copy protection technique to not just the IEEE 1394 but also the other network that is interconnected with the IEEE 1394.

[0011] It is another object of the present invention to provide a relay device and a communication device capable of realizing the contents protection procedure between devices that are not connected to the same network.

[0012] According to one aspect of the present invention there is provided a relay device, comprising: a first interface unit connected to a first network; a second interface unit connected to a second network; a proxy configuration unit for disclosing a device/service/sub-unit on the second network as an own device/service/sub-unit provided on the relay device with respect to a first network side; a control command reception unit for receiving control command signals destined to the own device/service/sub-unit from the first network side; a control command transmission unit for transmitting signals corresponding to the control command signals received by the control command reception unit, to the device/service/sub-unit on the second network; a contents protection information reception unit for receiving contents protection information destined to the own device/service/sub-unit, from a device on the first network; and a contents protection information transfer unit for transferring the contents protection information received by the contents protection information reception unit to the device/service/sub-unit on the second network, without making any change in the contents protection information.

[0013] According to another aspect of the present invention there is provided a relay device, comprising: a first interface unit connected to a first network; a second interface unit connected to a second network; a proxy configuration unit for disclosing each device/service/sub-unit on the first network or the second network as an own device/service/sub-unit provided on the relay device with respect to respective another network side; a control command reception unit for receiving control command signals destined to the own device/service/sub-unit from a side of one network to which the own device/service/sub-unit is disclosed by the proxy configuration unit; a control command transmission unit for transmitting signals corresponding to the control command signals received by the control command reception unit, to said each device/service/sub-unit on another network different from said one network; a contents protection information reception unit for receiving contents protection information destined to the own device/service/sub-unit from a device on the first network or the second network; a contents protection information transfer unit for transferring the contents protection information received by the contents

protection information reception unit to said each device/service/sub-unit on said another network, without making any change in the contents protection information; a contents reception unit for receiving contents destined to the own device/service/sub-unit and protected by a contents key obtained from the contents protection information, from a device on the first network or the second network; and a contents transfer unit for transferring the contents received by the contents reception unit to said each device/service/sub-unit on said another network, without making any change in the contents.

[0014] In this relay device, the contents protection information can be information related to a contents protection procedure including an authentication and/or a key exchange between one device/service/sub-unit on the first network and another device/service/sub-unit on the second network.

[0015] According to this aspect of the present invention, between "a device/service/sub-unit on the second network that is provided by the proxy configuration unit" and "a device on the first network" which are a pair that is carrying out transmission or reception of contents to be protected, for example, "a device on the first network" or "a device/service/sub-unit on the second network that is provided by the proxy configuration unit" can carry out the contents protection procedure while recognizing the target of the contents protection procedure as this relay device, so that there is no need for "a device on the first network" or "a device/service/sub-unit on the second network that is provided by the proxy configuration unit" to account for the other network that is connected via the relay device. Also, the relay device actually relays this procedure without changing its content, so that this contents protection procedure can be carried out directly between "a device/service/sub-unit on the second network that is provided by the proxy configuration unit" and "a device on the first network".

[0016] Also, according to this aspect of the present invention, the contents to be protected can be delivered to the receiving side without changing their protection format, so that the contents can be delivered end-to-end in the protected form.

[0017] According to another aspect of the present invention there is provided a relay device, comprising: a first interface unit connected to a first network; a second interface unit connected to a second network; a proxy configuration unit for disclosing each device/service/sub-unit on the first network or the second network as an own device/service/sub-unit provided on the relay device with respect to respective another network side; a control command reception unit for receiving control command signals destined to the own device/service/sub-unit from a side of one network to which the own device/service/sub-unit is disclosed by the proxy configuration unit; a control command transmission unit for transmitting signals corresponding to the control command signals received by the control command reception unit, to said each device/service/sub-unit on another network different from said one network; a first contents protection unit for carrying out a contents protection procedure with respect to one device/service/sub-unit on the first network; a second contents protection unit for carrying out the contents protection procedure with respect to another device/service/sub-unit on the second network; a contents reception unit for receiving contents destined to the own device/service/sub-unit and encrypted according to one of the first and second contents protection units; and a contents transfer unit for transferring the contents received by the contents reception unit to said each device/service/sub-unit on said another network, by encrypting the contents according to another one of the first and second contents protection units.

[0018] According to this aspect of the present invention, between "a device/service/sub-unit on the second network" and "a device on the first network" which are a pair that is carrying out transmission or reception of contents to be protected, for example, "a device on the first network" or "a device/service/sub-unit on the second network" can carry out the contents protection procedure while recognizing the target of the contents protection procedure as this relay device, so that there is no need for "a device on the first network" or "a device/service/sub-unit on the second network" to account for the other network that is connected via the relay device. Also, the relay device terminates each contents protection procedure so that the contents protection procedure is carried out separately between "a device/service/sub-unit on the second network" and the relay device, and between the relay device and "a device on the first network", for example, and therefore it becomes possible to carry out the contents protection end-to-end.

[0019] Also, according to this aspect of the present invention, data to be transferred are encrypted throughout the entire route between "a device on the first network" or "a device/service/sub-unit on the second network", so that it becomes possible to prevent the illegal copy or the like.

[0020] In this relay device, the first contents protection unit and the second contents protection unit can use different encryption schemes or identical encryption scheme based on different key information.

[0021] Also, in this relay device, the contents reception unit and the contents transmission unit can be sealed within a single LSI. In this way, even though the non-encrypted contents data will flow between the decryption unit and the encryption unit, but it becomes possible to prevent the illegal copy by eavesdropping the contents data from there, by attaching a probe individually, for example.

[0022] Also, in this relay device, a first key information used in the contents protection procedure in the first contents protection unit and a second key information used in the contents protection procedure in the second contents protection unit can be set to be identical. In this way, the information notified from one network regarding a key of the encrypted data that are transferred to another network (key, seed, etc.) can be directly transferred to another network such that it becomes possible for a device on another network to reproduce the encryption key, so that there is no need for the decryption function and the re-encryption function between the contents reception unit and the contents transmission unit, and therefore it becomes possible to realize a considerable reduction of a cost and a faster processing speed for the relay device.

[0023] Also, in this relay device, the contents protection procedure in said another one of the first and second contents protection units can be carried out in units of contents/services/sub-units, using a prescribed key information. In this way, it becomes possible to define a plurality of encryption keys between the relay device and a device on another network side, so that it becomes possible to transfer the encrypted data simultaneously, and it becomes possible to deal with the case where a plurality of encrypted data are transferred from a device on one network or the case where there are a plurality of devices on one network.

[0024] Also, this relay device can further comprise a configuration information reception unit for receiving a configuration information from one device/service/sub-unit on the first network or the second network, the configuration information indicating at least a presence or absence of an authentication format for said one device/service/sub-unit; and a configuration recognition unit for recognizing a configuration of said one device/service/sub-unit according to the configuration information received by the configuration information reception unit. In this way, the proxy services to be configured by the proxy configuration unit can be configured automatically, so that it becomes possible to realize the procedure up to the contents protection procedure in a plug-and-play fashion.

[0025] According to another aspect of the present invention there is provided a relay device, comprising: a first interface unit connected to a first network; a second interface unit connected to a second network; a first contents protection unit for carrying out a contents protection procedure with respect to one device/service/sub-unit on the first network; a second contents protection unit for carrying out the contents protection procedure with respect to another device/service/sub-unit on the second network; a contents

reception unit for receiving contents destined to an own device/service/sub-unit on the relay device and encrypted according to one of the first and second contents protection units, from a device on one of the first network and the second network; and a contents transmission unit for transmitting the contents received by the contents reception unit to a device/service/sub-unit on another one of the first network and the second network, by encrypting the contents according to another one of the first and second contents protection units; wherein a first key information used in the contents protection procedure in the first contents protection unit and a second key information used in the contents protection procedure in the second contents protection unit are set to be identical.

[0026] According to another aspect of the present invention there is provided a communication device, comprising: an interface unit connected to a network; a copy protection processing unit for carrying out a prescribed contents protection procedure including at least an authentication procedure and/or a key exchange procedure, with respect to another device/service/sub-unit on the network; a contents transmission unit for transmitting encrypted contents to which an address of the communication device is attached, either through a virtual channel on the network or by further attaching an identifier by which the encrypted contents can be uniquely identified by the communication device, to another device on the network; a reception unit for receiving a query regarding a service/sub-unit/plug that is transferring the encrypted contents either through the virtual channel or by attaching the identifier, from said another device on the network; and a notification unit for notifying a service/sub-unit/plug that is transferring the encrypted contents, to said another device on the network in response to the query.

[0027] According to another aspect of the present invention there is provided a communication device, comprising: an interface unit connected to a network; a copy protection processing unit for carrying out a prescribed contents protection procedure including at least an authentication procedure and/or a key exchange procedure, with respect to another device/service/sub-unit on the network; a contents reception unit for receiving encrypted contents to which an address of another device on the network is attached, either through a virtual channel on the network or in a form having an identifier by which the encrypted contents can be uniquely identified by said another device further attached thereto, from said another device; a transmission unit for transmitting a query regarding a service/sub-unit/plug that is transferring the encrypted contents either through the virtual channel or by attaching the identifier, to said another device on the network; and a reception unit for receiving a notification regarding a service/sub-unit/plug that is transferring the encrypted contents, from said another device in response to the query.

[0028] According to this aspect of the present invention, it becomes possible to specify a sub-unit or a plug that is transmitting or receiving the encrypted data that are transferred through a specific virtual channel, and it becomes possible to explicitly indicate that the authentication and key exchange regarding data transmitted or received from this sub-unit (or plug) should be carried out in the subsequent authentication and key exchange, so that it becomes possible to define a plurality of keys simultaneously even between the same nodes and therefore the exchange of a plurality of encrypted data becomes possible.

[0029] Else, according to this aspect of the present invention, it becomes possible to specify a sub-unit or a plug that is transmitting or receiving the encrypted data that are transferred with a specific identifier attached thereto, and it becomes possible to explicitly indicate that the authentication and key exchange regarding data transmitted or received from this sub-unit (or plug) should be carried out in the subsequent authentication and key exchange, so that it becomes possible to define a plurality of keys simultaneously even between the same nodes and therefore the exchange of a plurality of encrypted data becomes possible.

[0030] According to another aspect of the present invention there is provided a communication device, comprising: an interface unit connected to a network; a contents transfer unit for transmitting or receiving encrypted contents with respect to another device on the network, through a flow identified by a set of a source address, a source port, a destination address, and a destination port; and a copy protection processing unit for carrying out a prescribed contents protection procedure including at least an authentication procedure and/or a key exchange procedure with respect to said another device, using a prescribed logical port, in units of the flow.

[0031] In this communication device, an identifier of the flow can be attached to information exchanged in at least a part of procedures included in the prescribed contents protection procedure.

[0032] According to this aspect of the present invention, it becomes possible to define different keys for different flows, and it becomes possible to explicitly indicate that the authentication and key exchange regarding data transmitted or received from this sub-unit (or plug) should be carried out in the subsequent authentication and key exchange, so that it becomes possible to define a plurality of keys simultaneously even between the same nodes and therefore the exchange of a plurality of encrypted data becomes possible.

[0033] According to another aspect of the present invention there is provided a communication device, comprising: an interface unit connected to a network; a copy protection processing unit for carrying out a prescribed contents protection procedure including at least an authentication procedure and/or a key exchange procedure, with respect to another device on the network; and a contents transmission and reception unit for transmitting or receiving encrypted contents to which an address of a transmitting side device is attached, either through a virtual channel on the network or in a form having an identifier by which the encrypted contents can be uniquely identified by said transmitting side device further attached thereto, with respect to said another device; wherein at least one of an identifier of a service, a sub-unit, a virtual channel, or a plug that carries out exchange of the encrypted contents, and an identifier by which the encrypted contents can be uniquely identified by said transmitting side device, is attached to information exchanged in at least a part of procedures included in the prescribed contents protection procedure.

[0034] According to this aspect of the present invention, it becomes possible to explicitly indicate that the authentication and key exchange regarding data transmitted or received from this sub-unit, plug, or virtual channel should be carried out in the authentication and key exchange, so that it becomes possible to define a plurality of keys simultaneously even between the same nodes and therefore the exchange of a plurality of encrypted data becomes possible.

[0035] Else, according to this aspect of the present invention, it becomes possible to explicitly indicate that the authentication and key exchange regarding data transmitted or received from this sub-unit or plug, or with the specific identifier attached thereto should be carried out in the authentication and key exchange, so that it becomes possible to define a plurality of keys simultaneously even between the same nodes and therefore the exchange of a plurality of encrypted data becomes possible.

[0036] According to another aspect of the present invention there is provided a relay device, comprising: a first interface unit connected to a first network; a second interface unit connected to a second network; a first copy protection processing unit for carrying out a prescribed contents protection procedure including at least an authentication procedure and a key exchange procedure, with respect to one device/service/sub-unit on the first network; a second copy protection processing unit for carrying out the prescribed contents protection procedure including at least an authentication procedure and a key exchange procedure, with

respect to another device/service/sub-unit on the second network; a contents reception unit for receiving encrypted data containing specific contents from the first interface unit; a decryption unit for decrypting the encrypted data receiving by the contents reception unit, by using a contents protection key provided by the first copy protection processing unit, to obtain decrypted data; a conversion unit for converting the decrypted data into converted data in another coding format; an encryption unit for encrypting the converted data, by using a contents protection key provided by the second copy protection processing unit, to obtain re-encrypted data; and a contents transmission unit for transferring the re-encrypted data to the second interface unit.

[0037] According to this aspect of the present invention, in the case where it is required to transfer data to the second network in a data format different from the original data, as in the case where data to be transmitted through the first network are contents to be protected and the communication bandwidths of the first network and the second network are largely different, the conversion of the data format can be carried out by the conversion unit while the data to be transferred are encrypted throughout the entire route between a device on the first network to a device/service/sub-unit on the second network, so that it becomes possible to prevent the illegal copy or the like at both sections (in both data formats).

[0038] This relay device can further comprise a proxy configuration unit for disclosing one device/service/sub-unit on the second network as one own device/service/sub-unit provided on the relay device with respect to a first network side, and transmitting to said one device/service/sub-unit on the second network an information having a content according to information destined to said one own device/service/sub-unit that is received from a device on the first network side, while also disclosing another device/service/sub-unit on the first network as another own device/service/sub-unit provided on the relay device with respect to a second network side, and transmitting to said another device/service/sub-unit on the first network an information having a content according to information destined to said another own device/service/sub-unit that is received from a device on the second network side, such that when the prescribed contents protection procedure between a device on one network among the first and second networks and a device/service/sub-unit on another network among the first and second networks is to be carried out, the proxy configuration unit carries out the prescribed contents protection procedure with the device on said one network by using one of the first and second copy protection processing units, while carrying out the prescribed contents protection procedure with the device/service/sub-unit on said another network by using another one of the first and second copy protection processing units.

[0039] According to this aspect of the present invention, between "a device/service/sub-unit on another network" and "a device on one network" which are a pair that is carrying out transmission or reception of contents to be protected, "a device on one network" or "a device/service/sub-unit on another network" can carry out the contents protection procedure while recognizing the target of the contents protection procedure as this relay device, so that there is no need for "a device on one network" or "a device/service/sub-unit on another network" to account for the other network that is connected via the relay device. Also, the relay device actually terminates each contents protection procedure so that the contents protection procedure is carried out separately between "a device/service/sub-unit on another network" and the relay device, and between the relay device and "a device on one network", and therefore it becomes possible to carry out the contents protection end-to-end.

[0040] According to another aspect of the present invention there is provided a relay device, comprising: a first interface unit connected to a first network; a second interface unit connected to a second network; a first contents protection unit for carrying out a contents protection procedure with respect to one device/service/sub-unit on the first network; a second contents protection unit for carrying out the contents protection procedure with respect to another device/service/sub-unit on the second network; a contents reception unit for receiving contents destined to an own device/service/sub-unit on the relay device and encrypted according to one of the first and second contents protection units, from a device on one of the first network and the second networks; and a contents transmission unit for transmitting the contents received by the contents reception unit to a device/service/sub-unit on another one of the first network and the second network, by encrypting the contents according to another one of the first and second contents protection units; wherein said one of the first and second contents protection units carries out an authentication and/or a key exchange with a device/service/sub-unit on said one of the first network and the second network by referring to a relationship between the contents reception unit and the contents transmission unit, when there is a request for a procedure of the authentication and/or the key exchange with respect to said another one of the first and second contents protection units.

[0041] Other features and advantages of the present invention will become apparent from the following description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0042] FIG. 1 is a schematic diagram showing an exemplary overall configuration of a network according to the first embodiment of the present invention.

[0043] FIG. 2 is a block diagram showing an exemplary internal configuration of a transmission node in the network of FIG. 1.

[0044] FIG. 3 is a block diagram showing an exemplary internal configuration of a relay node in the network of FIG. 1.

[0045] FIG. 4 is a block diagram showing an exemplary internal configuration of a radio node in the network of FIG. 1.

[0046] FIG. 5 is a sequence chart showing an exemplary overall sequence in the first embodiment of the present invention.

[0047] FIG. 6 is another sequence chart showing an exemplary overall sequence in the first embodiment of the present invention.

[0048] FIG. 7 is a flow chart showing an exemplary operation procedure of a transmission node according to the first embodiment of the present invention.

[0049] FIG. 8 is another flow chart showing an exemplary operation procedure of a transmission node according to the first embodiment of the present invention.

[0050] FIG. 9 is a flow chart showing an exemplary operation procedure of a relay node according to the first embodiment of the present invention.

[0051] FIG. 10 is another flow chart showing an exemplary operation procedure of a relay node according to the first embodiment of the present invention.

[0052] FIG. 11 is another flow chart showing an exemplary operation procedure of a relay node according to the first embodiment of the present invention.

[0053] FIG. 12 is a flow chart showing an exemplary operation procedure of a radio node according to the first embodiment of the present invention.

[0054] FIG. 13 is another flow chart showing an exemplary operation procedure of a radio node according to the first embodiment of the present invention.

[0055] FIG. 14 is a diagram showing an exemplary format of a radio node configuration information packet used in the first embodiment of the present invention.
[0056] FIG. 15 is a diagram showing an exemplary form of a proxy table used in the first embodiment of the present invention.
[0057] FIG. 16 is another diagram showing an exemplary form of a proxy table used in the first embodiment of the present invention.
[0058] FIG. 17 is a diagram showing an internal configuration of a relay node as seen from a transmission node in the network of FIG. 1.
[0059] FIG. 18 is a diagram showing an internal configuration of a relay node as seen from a radio node in the network of FIG. 1.
[0060] FIG. 19 is a diagram showing an exemplary format of a radio node control packet used in the first embodiment of the present invention.
[0061] FIG. 20 is a schematic diagram showing an exemplary overall configuration of a network according to the second embodiment of the present invention.
[0062] FIG. 21 is a block diagram showing an exemplary internal configuration of a transmission node in the network of FIG. 20.
[0063] FIG. 22 is a block diagram showing an exemplary internal configuration of a relay node in the network of FIG. 20.
[0064] FIG. 23 is a block diagram showing an exemplary internal configuration of a radio node in the network of FIG. 20.
[0065] FIG. 24 is a sequence chart showing an exemplary overall sequence in the second embodiment of the present invention.
[0066] FIG. 25 is another sequence chart showing an exemplary overall sequence in the second embodiment of the present invention.
[0067] FIG. 26 is a flow chart showing an exemplary operation procedure of a transmission node according to the second embodiment of the present invention.
[0068] FIG. 27 is another flow chart showing an exemplary operation procedure of a transmission node according to the second embodiment of the present invention.
[0069] FIG. 28 is a flow chart showing an exemplary operation procedure of a relay node according to the second embodiment of the present invention.
[0070] FIG. 29 is another flow chart showing an exemplary operation procedure of a relay node according to the second embodiment of the present invention.
[0071] FIG. 30 is another flow chart showing an exemplary operation procedure of a relay node according to the second embodiment of the present invention.
[0072] FIG. 31 is another flow chart showing an exemplary operation procedure of a relay node according to the second embodiment of the present invention.
[0073] FIG. 32 is a flow chart showing an exemplary operation procedure of a radio node according to the second embodiment of the present invention.
[0074] FIG. 33 is another flow chart showing an exemplary operation procedure of a radio node according to the second embodiment of the present invention.
[0075] FIG. 34 is a diagram showing an exemplary form of a proxy table used in the second embodiment of the present invention.
[0076] FIG. 35 is another diagram showing an exemplary form of a proxy table used in the second embodiment of the present invention.
[0077] FIG. 36 is a diagram showing an internal configuration of a relay node as seen from a transmission node in the network of FIG. 20.
[0078] FIG. 37 is a diagram showing an internal configuration of a relay node as seen from a radio node in the network of FIG. 20.
[0079] FIG. 38 is a diagram showing an exemplary format of a radio frame used in the second embodiment of the present invention.
[0080] FIG. 39 is a diagram showing an exemplary format of a radio node control packet used in the second embodiment of the present invention.
[0081] FIG. 40 is a schematic diagram showing an exemplary overall configuration of a network according to the third embodiment of the present invention.
[0082] FIG. 41 is a block diagram showing an exemplary internal configuration of a transmission node in the network of FIG. 40.
[0083] FIG. 42 is a block diagram showing an exemplary internal configuration of a home gateway in the network of FIG. 40.
[0084] FIG. 43 is a block diagram showing an exemplary internal configuration of a reception node in the network of FIG. 40.
[0085] FIG. 44 is a sequence chart showing an exemplary overall sequence in the third embodiment of the present invention.
[0086] FIG. 45 is another sequence chart showing an exemplary overall sequence in the third embodiment of the present invention.
[0087] FIG. 46 is a flow chart showing an exemplary operation procedure of a transmission node according to the third embodiment of the present invention.
[0088] FIG. 47 is another flow chart showing an exemplary operation procedure of a transmission node according to the third embodiment of the present invention.
[0089] FIG. 48 is a flow chart showing an exemplary operation procedure of a home gateway according to the third embodiment of the present invention.
[0090] FIG. 49 is another flow chart showing an exemplary operation procedure of a home gateway according to the third embodiment of the present invention.
[0091] FIG. 50 is another flow chart showing an exemplary operation procedure of a home gateway according to the third embodiment of the present invention.
[0092] FIG. 51 is another flow chart showing an exemplary operation procedure of a home gateway according to the third embodiment of the present invention.
[0093] FIG. 52 is a flow chart showing an exemplary operation procedure of a reception node according to the third embodiment of the present invention.
[0094] FIG. 53 is another flow chart showing an exemplary operation procedure of a reception node according to the third embodiment of the present invention.
[0095] FIG. 54 is a diagram showing exemplary forms of a panel of a transmission node and a home page for transmission node control of a home gateway used in the third embodiment of the present invention.
[0096] FIG. 55 is a schematic diagram showing an exemplary overall configuration of a network according to the fourth embodiment of the present invention.
[0097] FIG. 56 is a block diagram showing an exemplary internal configuration of a transmission node in the

network of FIG. 55.
[0098] FIG. 57 is a block diagram showing an exemplary internal configuration of a relay node in the network of FIG. 55.
[0099] FIG. 58 is a block diagram showing an exemplary internal configuration of a radio node in the network of FIG. 55.
[0100] FIG. 59 is a sequence chart showing an exemplary overall sequence in the fourth embodiment of the present invention.
[0101] FIG. 60 is a flow chart showing an exemplary operation procedure of a transmission node according to the fourth embodiment of the present invention.
[0102] FIG. 61 is a flow chart showing an exemplary operation procedure of a relay node according to the fourth embodiment of the present invention.
[0103] FIG. 62 is another flow chart showing an exemplary operation procedure of a relay node according to the fourth embodiment of the present invention.
[0104] FIG. 63 is a flow chart showing an exemplary operation procedure of a radio node according to the fourth embodiment of the present invention.
[0105] FIG. 64 is another flow chart showing an exemplary operation procedure of a radio node according to the fourth embodiment of the present invention.
[0106] FIG. 65 is a schematic diagram showing an exemplary overall configuration of a network according to the fifth embodiment of the present invention.
[0107] FIG. 66 is a flow chart showing an exemplary operation procedure of a relay node according to the fifth embodiment of the present invention.
[0108] FIG. 67 is a sequence chart showing an exemplary overall sequence in the fifth embodiment of the present invention.
[0109] FIG. 68 is another sequence chart showing an exemplary overall sequence in the fifth embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

First Embodiment

[0110] Referring now to FIG. 1 to FIG. 19, the first embodiment of a relay device and a communication device according to the present invention will be described in detail.
[0111] FIG. 1 shows an exemplary overall configuration of a home network at some home. To this home network, three nodes including a transmission node 101, a relay node 102, and a radio node 103 are connected, where the transmission node 101 and the relay node 102 are connected to a (wire) IEEE 1394 bus 104 while the relay node 102 and the radio node 103 are connected to a radio network. Note however that it is made possible to carry out communications among these three nodes by the method described below.
[0112] In this embodiment, the exemplary case where MPEG video transmitted from the transmission node 101 is relayed at the relay node 102 and transmitted to the radio node 103 via the radio section will be described. In this exemplary case, encryption of the MPEG video data transferred between the transmission node 101 and the radio node 103 for the purpose of copyright protection (illegal copy prevention) will be considered.
[0113] Note that FIG. 1 shows three nodes, but any nodes other than these three nodes may also be connected (this also applies to all the other embodiments described below).
[0114] FIG. 2 shows an exemplary internal configuration of the transmission node 101.
[0115] The transmission node 101 is a device for storing the MPEG video data therein, which transmits the MPEG video data through the IEEE 1394 bus 104 according to the need. The transmission node 101 has a function for encrypting the MPEG video data to be transmitted whenever necessary, in order to prevent the illegal copying on the IEEE 1394 bus at a time of transmission. In addition, the transmission node 101 also has a function for carrying out exchange of authentication data, encryption key, etc., with a receiving node of the MPEG video data.
[0116] As shown in FIG. 2, this transmission node 101 comprises an IEEE 1394 interface 401, an AV/C protocol processing unit 402 for carrying out AV/C protocol processing, a copy protection processing unit 403 for carrying out processing regarding the copy protection within the AV/C protocol, an ISO signal transmission and reception unit 404 for transmitting and receiving data to be exchanged through isochronous channels among data transmitted and received through the IEEE 1394, an MPEG storage unit 406 for storing MPEG video data, and an encryption unit 405 for encrypting the MPEG video data by using an encryption key K given from the copy protection unit 403, and sending the encrypted MPEG video data to the ISO signal transmission and reception unit 404. Here, the copy protection unit 403 has an authentication format (device certificate) Acert.
[0117] Next, FIG. 3 shows an exemplary internal configuration of the relay node 102.
[0118] The relay node 102 has a function for forwarding data (MPEG video data) received from the IEEE 1394 bus side to the radio section side, a function for providing functions of the radio node as a proxy server of the radio node with respect to a node on the IEEE 1394 bus side, and a function for providing functions of a node on the IEEE 1394 bus side as a proxy server of a node on the IEEE 1394 bus side (the transmission node 101 in this embodiment) with respect to a node on the radio section side.
[0119] As shown in FIG. 3, this relay node 102 comprises an IEEE 1394 interface 201, a radio interface 202, an AV/C protocol processing unit 203, an ISO signal transmission and reception unit 204, a radio ISO signal transmission and reception unit 205 for transmitting and receiving signals of isochronous channels on the radio section side, a 1394 bus configuration recognition unit 206 having a function for collecting a configuration information of a node on the IEEE 1394 bus and advertising the own configuration information (such as information regarding functions that are provided by the own device) on the IEEE 1394, a proxy sub-unit configuration unit 207 for disclosing a node and services (sub-units) on the radio section side with respect to the IEEE 1394 bus side as a proxy, accepting commands and the like for a node and services on the radio section side as a proxy and transmitting them to the radio section side by applying a protocol conversion according to the need, or disclosing a node and services (sub-units) on the IEEE 1394 side with respect to the radio section side as a proxy, accepting commands and the like for a node and services on the IEEE 1394 side as a proxy and transmitting them to the IEEE 1394 side by applying a protocol conversion according to the need, a radio section configuration recognition unit 209 having a function for collecting a configuration information of a node on the radio section and advertising the own configuration information (such as information regarding functions that are provided by the own device) on the radio section, a copy protection control/forward unit 210 for carrying out processing regarding the copy protection and transparently forwarding information to be exchanged regarding the copy protection processing across the 1394 bus and the radio section, and a radio node control packet transmission and reception unit 211 for transmitting and receiving control packets to be exchanged in the radio section.

[0120] Next, FIG. 4 shows an exemplary internal configuration of the radio node 103.
[0121] In the radio section, there is no need to have the so called IEEE 1394 protocol (physical layer protocol, link layer protocol, etc.) activated, and arbitrary radio protocol such as the IEEE 802.11, radio LAN, etc., can be used, but in this embodiment, it is assumed that a radio network having the so called QOS function (isochronous communication function) is to be used. Note however that this embodiment is not limited to the case where the QOS function is required in the radio section.
[0122] In order for the radio node 103 that is not the so called IEEE 1394 node to carry out communications with a node (the transmission node 101 in this embodiment) connected to the IEEE 1394 bus, the relay node 102 emulates a node and functions (sub-units) on the IEEE 1394 bus as mentioned above. Namely, from a viewpoint of the radio node 103, the relay node 102 functions as the so called proxy server for a node and functions on the IEEE 1394 bus side. The radio node 103 carries out communications by regarding these node and functions on the IEEE 1394 side as functions of the relay node 102 but in reality the relay node 102 carries out the necessary protocol conversion and data transfer.
[0123] As shown in FIG. 4, this radio node 103 comprises a radio interface 301, a radio node control packet transmission and reception unit 302, a copy protection processing unit 303, a radio ISO signal transmission and reception unit 304, a decryption unit 305 for decrypting the received encrypted stream (MPEG video, etc.) by using the contents key K given from the copy protection unit 303, an MPEG decoding unit 306, and a display unit 307 for displaying video.
[0124] As will be described below, the copy protection unit 303 of the radio node 103 has an authentication format (device certificate) Bcert, which is issued by the same issuance organization that issued the authentication format Acert of (the video transmission sub-unit of) the transmission node 101.
[0125] Next, the actual operation sequence for the entire MPEG video transmission after applying the copy protection will be described with references to an exemplary overall sequence shown in FIGS. 5 and 6, an exemplary flow chart for the transmission node 101 shown in FIGS. 7 and 8, an exemplary flow chart for the relay node 102 shown in FIGS. 9, 10 and 11, and an exemplary flow chart for the radio node 103 shown in FIGS. 12 and 13.
[0126] First, the radio node 103 notifies the own configuration information to the relay node 102 (step S501). This notification may be carried out by providing an IEEE 1212 register within the radio node and registering the own configuration information therein. The configuration information indicates that the own node (radio node) has the MPEG decoding/display function, the authentication format (device certificate) for the authentication and key exchange purpose, etc. Here, the fact that this authentication format (device certificate) is a format defined by the specific copy protection organization, or the fact that it is the authentication format (device certificate) for the copy protection of the IEEE 1394, may also be notified at the same time.
[0127] Now, the authentication will be described briefly.
[0128] When contents (data) such as movies or TV programs for which the copyright should be taken into consideration are to be transferred on the network, these contents should be protected by the encryption, because the illegal copy would become possible if these data are eavesdropped on the network during data transfer. As a measure against the eavesdropping, the encryption of data to be transferred is effective.
[0129] Another problem is whether there is a possibility of transmitting data to someone untrustworthy. For example, even in the case of transmitting data in an encrypted form, data should not be transmitted in a form that enables the cryptoanalysis in the case where the destination node (which has a key for decrypting the encryption) is a malicious one (that has an intention to make the illegal copy). The authentication is the measure against this problem. Namely, it is a mechanism which verifies that the receiving side is someone who does not commit any illegal act, before giving a key for decrypting the encryption to the receiving side (and the key for decrypting the encryption is given only to the receiving side node for which the above fact is verified).
[0130] More specifically, data called "authentication format (device certificate)" are given in advance to those nodes (or sub-units) that are verified as "a node (or sub-unit) that does not commit any illegal act" by the authentication organization in advance. The fact that a node (or sub-unit) has this "authentication format (device certificate)" in a correct form implies that this node (or sub-unit) can be regarded as trustworthy (one that does not commit any illegal act). For this reason, the exchange of the authentication format (device certificate) is carried out between the transmitting and receiving nodes (or sub-units) prior to the above described data transfer, and the key for decrypting the encryption (or data that is a seed for generating the key) is notified only in the case where the authentication format (device certificate) is verified as being in a correct form, and data encrypted by using that key are transferred on the network.
[0131] Now, the radio node 103 is given such an authentication format (device certificate) from the authentication organization in advance, and has a "right to receive/playback encrypted data in appropriate form" Here, the authentication format (device certificate) possessed by the radio node 103 is assumed to be "Bcert".
[0132] The radio node 103 may add the fact that the own node has the authentication format (device certificate), to the configuration information at a time of notifying the own configuration information at the step S501 of FIG. 5 (step S801). For example, as shown in FIG. 14, the configuration information may contain information that this radio node 103 has the MPEG decoding/display function, that this function has the authentication format (device certificate), that this authentication format (device certificate) is issued by so and so issuance organization, etc.
[0133] Note that, as a method by which the relay node 102 recognizes the configuration of the radio node 103, it is also possible to use a method in which the relay node 102 transmits a packet for inquiring the configuration to the radio node 103, and the radio node 103 responds to this query, instead of the above described method.
[0134] Now, the relay node 102 that received this configuration information checks that the radio node 103 has the authentication format (device certificate) and the MPEG decoding/display function (step S701).
[0135] In order to notify that the radio node 103 has the MPEG decoding/display function to a node on the IEEE 1394 bus side, the relay node 102 advertises this MPEG decoding/display function as the own sub-unit of the relay node 102 to the IEEE 1394 bus side (step S502). More specifically, the relay node 102 registers that "the own node has the MPEG decoding/display function" in the IEEE 1212 register, or returns a reply indicating that the own node has the MPEG decoding/display sub-unit upon receiving a query regarding the sub-unit configuration by the AV/C protocol (such that a node connected to the IEEE 1394 recognizes that this function exists in the relay node 102).
[0136] To this end, the relay node 102 has a proxy table 208 inside the proxy sub-unit configuration unit 207. The proxy table 208 is a table registering the correspondence between a form in which the relay node 102 is advertising as a proxy and its actual substance, as shown in FIGS. 15 and 16.
[0137] Here, the MPEG decoding/display function of the radio node 103 is advertised as the sub-unit of the relay node, as shown in FIG. 15 (steps S702, S703).
[0138] As a result, the structure of the relay node 102 as seen from the transmission node 101 appears as

shown in FIG. 17 (step S601).
[0139] The above description is directed to the IEEE 1394 bus side, but the same relationship also holds in the radio section. Namely, the relay node 102 surveys instruments, services, sub-unit configuration, etc. on the IEEE 1394 bus side and provides their proxy services with respect to the radio section side. As a result, the setting as shown in FIG. 16 is made and the structure of the relay node 102 as seen from the radio node appears as shown in FIG. 18.
[0140] Now, the transmission node 101 that recognized that there is an MPEG decoding/display sub-unit in the relay node 102 establishes an isochronous channel #x on the 1394 bus and issues a command of "connect (a plug (a plug in the AV/C as specified by the 1394 TA, for example) for receiving) this isochronous channel #x with the MPEG decoding/display sub-unit, and display the video" in the AV/C protocol (steps S503, S602), for the purpose of transferring the MPEG video to this sub-unit. The transmission node 101 interprets that this sub-unit exists in the relay node 102 so that the destination of the command is the relay node 102.
[0141] The relay node 102 that received this command (step S704) interprets the received command packet, recognizes that this command is a command with respect to the MPEG decoding/display sub-unit for which the proxy service is provided by the own node, refers to the proxy table 208, and recognizes that the substance to which this command is directed exists in the radio node 103 (step S705).
[0142] Consequently, in order to forward data received through the isochronous channel #x of the IEEE 1394 bus to the radio node side, the isochronous channel (#y) in the radio section is reserved (step S706), and the ISO signal transmission and reception unit 204 (that receives the isochronous channel #x) and the radio ISO signal transmission and reception unit 205 (that transmits the isochronous channel #y) are connected, such that the input data (ISO data) entered from the 1394 interface 201 can be forwarded to the radio section (steps S504, S707).
[0143] In addition, a command "data will be transmitted through the radio isochronous channel #y so that receive them, enter them into an MPEG decoder, and display the decoding result on a display" is transmitted to the radio node 103 in a form of a radio node control packet (steps S505, S708).
[0144] FIG. 19 shows an exemplary format of this radio node control packet.
[0145] As shown in FIG. 19, this packet has a content that urges the radio node 103 to transfer data (MPEG video) received through the radio isochronous channel #y to the MPEG decoding/display function and display them. In addition, information regarding the sub-unit (the video transmission function of the relay node 102; actually, it advertises as having this function as a proxy for the transmission node 101) that transmits this data (MPEG video) is also notified in this packet. (That is, the source of the data is notified in this packet.)
[0146] The radio node 103 that received this packet recognizes that data will be transmitted through the radio isochronous channel #y (step S802). The radio node 103 recognizes the source of these data as the video transmission sub-unit of the relay node 102 (actually, the data source is the transmission node 101, as mentioned above). For this reason, information indicating that "the source of data transmitted through this radio isochronous channel is the video transmission sub-unit of the relay node 102" may also be included in this radio node control packet.
[0147] After that, the transmission node 101 transfers the encrypted MPEG video through the isochronous channel #x (steps S603, S506). The relay node 102 that received these data forwards them to the radio section, as has been set up previously (steps 709, S507).
[0148] The relay node 102 can recognize that received data are encrypted data when the encrypted MPEG video data are received at the step S506, but it recognizes that there is a need to transfer them to the radio network side so that it forwards them as they are. It may also memorize the fact that the authentication and key exchange procedure is necessary later on.
[0149] In this way, the encrypted MPEG video reaches to the radio node 103 (step S803). This MPEG video may contain a node ID of the relay node 102 as the source address. For this reason, the radio node 103 can recognize that this MPEG video has arrived from the relay node 102, but as the radio node 103 does not have the key K for decrypting the encryption (or data that is a seed for generating that key) at this point, it cannot decrypt the encryption and take out the original MPEG video in this state. At this point, the radio node 103 recognizes that the authentication procedure with the source of the MPEG video is necessary.
[0150] Consequently, (the copy protection processing unit 303 of) the radio node 103 transmits the authentication request to the source of the encrypted data. As already mentioned above, the radio node 103 recognizes (a sub-unit with a sub-unit type=video transmission sub-unit and a sub-unit ID=b (where b=0) within) the relay node 102 as the source of the encrypted data.
[0151] Also, as in S521 of FIG. 5, a query "A sub-unit with the sub-unit type=MPEG decoding/display sub-unit and the sub-unit ID=c (where c=0) is receiving the radio isochronous channel #y at the radio node. Which sub-unit is transmitting the encrypted data to the radio isochronous channel #y?" may be transmitted to the relay node 102. In response, the relay node 102 returns a reply "A sub-unit ID=0 of the video transmission sub-unit is transmitting to the radio isochronous channel #y" (steps S522, S731, S831). In this way, the radio node 103 can recognize that the target of the authentication is the video transmission sub-unit of the relay node 102.
[0152] In this way, the destination of the authentication request is recognized and the authentication request is transmitted to (a sub-unit ID=0 of the video transmission sub-unit within) the relay node 102. In this transmission, the destination of the authentication request packet may be set as "(a sub-unit ID=0 of) the video transmission sub-unit of the relay node", or information indicating "(a sub-unit ID=0 of) the video transmission sub-unit" may be entered at arbitrary position in the authentication request packet so as to explicitly indicate that the authentication request target is (a sub-unit ID=0 of) the video transmission sub-unit. In the former case, it implies that the authentication and key exchange procedure is contained in each sub-unit of the relay node. In the latter case, it implies that a specific processing unit provided in the relay node carries out the authentication and key exchange for all sub-units collectively.
[0153] At that point, the authentication format (device certificate) Bcert of the radio node 103 is attached to the authentication request (step S804, S508). This Bcert may be the authentication format (device certificate) of the MPEG decoding/display sub-unit of the radio node 103. Note that the copy protection processing unit may provide the authentication format (device certificate) for each sub-unit ID instead of that for each sub-unit (each sub-unit type).
[0154] The relay node 102 that received the authentication-request (step S710) refers to the proxy table 208 and recognizes that the request target of this authentication request is actually (a sub-unit ID=a (where a=0) of the video transmission sub-unit of) the transmission node 101.
[0155] The relay node 102 may transmit a query "A sub-unit ID=0 of the MPEG decoding/display sub-unit is receiving the isochronous channel #x at the relay node. Which sub-unit of the transmission node is transmitting the encrypted data to the isochronous channel #x?" to the transmission node 101 (steps S525, S631, S732). In response, the transmission node 101 returns a reply "A sub-unit ID=0 of the video transmission sub-unit is transmitting to the isochronous channel #x" (steps S524, S631, S732).

[0156] In this way, when the partner of the authentication request is recognized, the authentication request received at the step S508 is forwarded to the transmission node 101 without changing its content (by leaving Bcert, etc. unchanged). Namely, the relay node can transparently transfers the destination address, the authentication format (device certificate) of sub-units other than the sub-unit that is the destination of the authentication request, etc.
[0157] At a time of transferring the authentication request, the destination of the authentication request packet may be set as (a sub-unit ID=0 of) the video transmission sub-unit, or information indicating that sub-unit may be entered at arbitrary position in the authentication request packet so as to explicitly indicate that the authentication request target is that sub-unit, as mentioned above.
[0158] Here, by forwarding the authentication request without changing its content, the authentication request reaches to the transmission node 101 in its original form, so that the actual authentication procedure will proceed between the transmission node 101 and the radio node 103, and moreover it is possible to carry out the above procedure without revealing information such as the value of the key that becomes apparent as a result of the authentication, with respect to the other nodes including the relay node 102.
[0159] The transmission node 101 that received the authentication request interprets this as the authentication request that comes from the MPEG decoding/display sub-unit of the relay node 102 (step S604). Then, an ID (Bdid) for identifying the MPEG decoding/display sub-unit of the radio node 103 is extracted from Bcert (step S605), and using this, the similar authentication request is attempted with respect to the source of the authentication request. However, the transmission node 101 is not aware that Bcert is the authentication format (device certificate) of the radio node 103 and regards it rather as the authentication format (device certificate) of (the MPEG decoding/display sub-unit of) the relay node 102.
[0160] This authentication request contains the authentication format (device certificate) Acert of (the video transmission sub-unit) of the transmission node 101 and Bdid. Here, the transmission node 101 interprets (the MPEG decoding/display sub-unit of) the relay node 102 as the source of the authentication request (step S509), so that the relay node 102 also becomes the destination of this authentication request (steps S606, S510).
[0161] The relay node 102 that received this (step S712) refers to the proxy table 208, recognizes that the actual request target of this authentication procedure is (the MPEG decoding/display function of) the radio node 103, and forwards this authentication request to the radio node 103 without changing its content (by leaving Acert, etc. unchanged) (steps S511, S713). The source of this authentication request is the relay node 102.
[0162] The radio node 103 that received this interprets that it is the authentication request that comes from the video transmission sub-unit of the relay node 102 (step S805). Then, an ID (Adid) for identifying the video transmission sub-unit of the transmission node 101 is extracted from Acert, and the remaining procedure necessary for the exchange of the authentication key is attempted with respect to the source of the authentication request. Note that, in this case, the radio node 103 is not aware that Acert is the authentication format (device certificate) of the transmission node 101, and regards it rather as the authentication format (device certificate) of (the video transmission sub-unit of) the relay node 102.
[0163] As the remaining procedure necessary for the exchange of the authentication key, the radio node 103 transmits a authentication and key exchange procedure packet to (a node that is interpreted by the radio node as) the source of the authentication request. In this authentication and key exchange procedure packet, a key exchange initial value, a signature, a device ID (Adid) of (the vide transmission sub-unit of) the transmission node that was contained in Acert, etc., are contained (step S806). Here, the radio node 103 is interpreting (the video transmission sub-unit of) the relay node 102 as the source of the authentication request (step S511) so that the relay node 102 also becomes the destination of this authentication request.
[0164] The relay node 102 that received this refers to the proxy table 208, recognizes that the actual request target of this authentication procedure is (the video transmission sub-unit of) the transmission node 101, and forwards this authentication procedure packet to the transmission node 101 without changing its content (steps S513, S714). The source of this packet is the relay node 102.
[0165] The procedure similar to this is also carried out along the direction of transmission node 101->relay node 102->radio node 103 (steps S514, S515, S609, S715, S807).
[0166] Each of the transmission node 101 and the radio node 103 that received this authentication procedure packet carries out the tampering check as to whether or not the received packet has been altered, the check as to whether or not the authentication format (device certificate) sent from the partner is a correct one, etc., and derives the common authentication key Kauth using the given value. This common authentication key Kauth is a key to be shared between (the video transmission sub-unit of) the transmission node and (the MPEG decoding/display function of) the radio node, and it becomes possible to share this key Kauth without revealing it to anyone other than these two (the transmission node 101 and the radio node 103) at this point (steps S607, S608, S808).
[0167] Using this authentication key Kauth, it becomes possible to calculate the contents key K for actually carrying out the MPEG stream encryption. The detailed procedure for this calculation will be omitted here, but it may be made such that the calculation of the contents key K becomes possible by separately sending a value of the exchange key or the seed from the transmission node 101 to the radio node 103 as in the copy protection scheme (5C scheme) of the IEEE 1394 (steps S518, S519).
[0168] In this way, the value of the contents key K can be shared between (the video transmission sub-unit of) the transmission node 101 and (the MPEG decoding/display function of) the radio node 103.
[0169] The transmission node 101 encrypts the MPEG video to be transmitted by using the contents key K at the encryption unit 405 (step S610), and transmits this to (the MPEG decoding/display sub-unit of) the relay node 102 through the isochronous channel #x of the 1394 bus (steps S516, S611).
[0170] The relay node 102 transmits the encrypted MPEG video that is transmitted from the transmission node 101 through the isochronous channel #x to the radio isochronous channel #y, from the ISO signal transmission and reception unit 204 through the radio ISO signal transmission and reception unit 205 (steps S517, S716).
[0171] The radio node 103 that received this decrypts the encrypted MPEG video by using the value of the contents key K (step S809, S810). The decrypted MPEG video data are then decoded by the MPEG decoding unit 306 (step S811) and decoded data are playbacked at the display unit 307 (step S812).
[0172] In this way, even in the interconnected environment where the proxy node exists between the 1394 bus and the radio network, it is possible to carry out the authentication procedure and the key exchange procedure between nodes (the transmission node 101 and the radio node 103 in this embodiment) end-to-end, and moreover it is devised such that its content cannot be known by the other nodes including the relay node 102. Also, in the transfer of data that require the contents protection such as the actual MPEG video, etc., data are encrypted throughout the entire route so that the copying is impossible and therefore the safe data transfer is possible. As a result, it becomes possible to carry out the data transfer that

accounts for the copy protection even in such an interconnected environment.
[0173] Note that, in this embodiment, the authentication procedure, the encryption key exchange procedure, etc. are carried out in units of sub-units of the nodes, but it is also possible to carry out these in units of radio nodes. An example for carrying out these in units of nodes will be described in the second embodiment which can be applied to this embodiment as well.
[0174] Also, in this embodiment, the procedure for the authentication and the key exchange is carried out after receiving the encrypted data, but this procedure may be carried out prior to the encrypted data receiving. For example, this procedure may be carried out at a time of activation of the device or corresponding application.

Second Embodiment
[0175] Referring now to FIG. 20 to FIG. 39, the second embodiment of a relay device and a communication device according to the present invention will be described in detail.
[0176] In the first embodiment, the authentication procedure and the key exchange procedure are directly carried out by the transmission node and the radio node. Namely, (the video transmission sub-unit of) the transmission node and (the MPEG decoding/display function of) the radio node directly carry out the mutual authentication, the encryption key exchange procedure and the encrypted data exchange. In this case, the relay node functions as a proxy of the MPEG decoding/display function of the radio node with respect to the transmission node, and as a proxy of the video transmission sub-unit of the transmission node with respect to the radio node, but in the above described authentication procedure and encrypted data exchange, the relay node simply forwards these data to a sub-unit or a function for which it is functioning as a proxy.
[0177] In contrast, in the second embodiment, an exemplary case of terminating the series of copy protection procedure, that is, the authentication procedure and the encrypted data exchange, at the relay node will be described. Namely, each copy protection procedure is closed between the transmission node and the relay node, and between the relay node and the radio node. In other words, the relay node of this embodiment also provides the proxy services with respect to the transmission node or the radio node, but for the copy protection, the relay node itself has the authentication format (device certificate) and the relay node itself terminates a responsibility for the encrypted MPEG data transfer in the 1394 bus section as well as the encrypted MPEG data transfer in the radio section.
[0178] FIG. 20 shows an exemplary overall configuration of a home network at some home, which is basically the same as in the first embodiment.
[0179] FIG. 21 shows an exemplary internal configuration of the transmission node 2101, which is also basically the same as in the first embodiment.
[0180] FIG. 22 shows an exemplary internal configuration of the relay node 2102. Similarly as in the first embodiment, the relay node 2102 has a function for providing functions of the radio node as a proxy server of the radio node with respect to a node on the IEEE 1394 bus side, and a function for providing functions of a node on the IEEE 1394 bus side as a proxy server of a node (the transmission node 2101 in this embodiment) on the IEEE 1394 bus side with respect to a node on the radio section side.
[0181] Also, the relay node 2102 has a function for forwarding data (MPEG video data) received from the IEEE 1394 bus side to the radio section side, but the relay node 2102 of the second embodiment differs from that of the first embodiment in that the procedure related to the copy protection such as authentication and data encryption, etc., is terminated at the relay node 2102 both in the IEEE 1394 bus section and in the radio section, an IEEE 1394 copy protection processing unit 2208 has the authentication format (device certificate) Bcert for the IEEE 1394 bus side, a radio section copy protection processing unit 2212 has the authentication format (device certificate) Ccert for the radio section side, and the encrypted data entered from the isochronous channel of the 1394 bus are processed by the sequence of reception at the ISO signal transmission reception unit 2203->decryption at the decryption unit 2204->re-encryption of the decrypted MPEG video at the encryption unit 2205->transmission as the radio isochronous signals at the radio ISO signal transmission and reception unit 2206.
[0182] The authentication format (device certificate) may be provided one for each IEEE 1394 interface or each radio section interface, or one for each sub-unit (including proxy) (for each sub-unit type).
[0183] Here, it is assumed that Acert and Bcert are the authentication formats (device certificates) that were issued by the same authentication organization (the authentication organization responsible for the IEEE 1394 copy protection), but the authentication formats (device certificates) of the radio section (Ccert and Dcert to be described below) may or may not be issued by the same authentication organization, so that the authentication formats (device certificates) issued by a different authentication organization that is responsible for the radio section may be used.
[0184] Next, FIG. 23 shows an exemplary internal configuration of the radio node 2103, which is basically the same as that of the first embodiment except that a copy protection processing unit 2303 has the authentication format (device certificate) Dcert for the radio section.
[0185] Next, the actual operation sequence for the entire MPEG video transmission after applying the copy protection will be described with references to an exemplary overall sequence shown in FIGS. 24 and 25, an exemplary flow chart for the transmission node 2101 shown in FIGS. 26 and 27, an exemplary flow chart for the relay node 2102 shown in FIGS. 28, 29, 30 and 31, and an exemplary flow chart for the radio node 2103 shown in FIGS. 32 and 33.
[0186] First, the radio node 2103 notifies the own configuration information to the relay node 2102 (step S2501). The configuration information indicates that the own node (radio node) has the MPEG decoding/display function, the authentication format (device certificate) for the authentication purpose, etc. Here, the fact that this authentication format (device certificate) is an authentication format (device certificate) for the radio section may also be notified (step S2801).
[0187] The relay node 2102 that received this configuration information checks that the radio node 2103 has the authentication format (device certificate) and the MPEG decoding/display function (step S2701). Similarly as in the first embodiment, the relay node 2102 advertises this MPEG decoding/display function as the own sub-unit of the relay node 2102 to the IEEE 1394 bus side (step S2502), using the IEEE 1212 register or the AV/C protocol, etc.
[0188] To this end, the relay node 2102 has a proxy table. 2214 inside the proxy sub-unit configuration unit 2210. The proxy table 2214 is basically similar to that of the first embodiment, which is a table registering the correspondence between a form in which the relay node 2102 is advertising as a proxy and its actual substance, as shown in FIGS. 35 and 36.
[0189] Here, the MPEG decoding/display function of the radio node 2103 is advertised as the sub-unit of the relay node, as shown in FIG. 34 (steps S2702, S2703).
[0190] As a result, the structure of the relay node 2102 as seen from the transmission node 2101 appears as shown in FIG. 36 (step S2601).
[0191] The above description is directed to the IEEE 1394 bus side, but the same relationship also holds in the radio section, similarly as in the first embodiment. Namely, the relay node 2102 surveys instruments,

services, sub-unit configuration, etc. on the IEEE 1394 bus side and provides their proxy services with respect to the radio section side. As a result, the setting as shown in FIG. 35 is made and the structure of the relay node 2102 as seen from the radio node appears as shown in FIG. 37.
[0192] Now, the transmission node 2101 that recognized that there is an MPEG decoding/display sub-unit in the relay node 2102 establishes an isochronous channel #x on the 1394 bus and issues a command of "connect (a plug for receiving) this isochronous channel #x with the MPEG decoding/display sub-unit, and display the video" in the AV/C protocol (steps S2503, S2602), for the purpose of transferring the MPEG video to this sub-unit. The transmission node 2101 interprets that this sub-unit exists in the relay node 2102 so that the destination of the command is the relay node 2102.
[0193] The relay node 2102 that received this command (step S2704) interprets the received command packet, recognizes that this command is a command with respect to the MPEG decoding/display sub-unit for which the proxy service is provided by the own node, refers to the proxy table 2210, and recognizes that the substance to which this command is directed exists in the radio node 2103 (step S2705).
[0194] Here, it is assumed that the radio section of FIG. 20 is a QOS compatible radio LAN which is capable of transferring data up to the destination without any quality degradation such as packet loss or delay as long as the prescribed procedure is followed. On this radio LAN, the data are transferred in forms of a radio frame having a format similar to the Ethernet frame, that is, a format of "source address, destination address, data" as shown in FIG. 38.
[0195] Here, in order to forward data received through the isochronous channel #x of the IEEE 1394 bus to the radio node side, the QOS set up in the radio section may be carried out, and the ISO signal transmission and reception unit 2203 (that receives the isochronous channel #x) and the radio ISO signal transmission and reception unit 2206 (that transmits the radio frames with guaranteed QOS) may be connected as indicated by a dashed line in FIG. 22 (because the decryption cannot be carried out yet), such that the ISO input data entered from the 1394 interface 2201 can be forwarded to the radio section as it is (steps S2504, S2706, S2707).
[0196] In addition, a command "data will be transmitted through the radio frames so that receive them, and display the result on a display" is transmitted to the radio node 103 in a form of a radio node control packet (steps S505, S708, S2802). For this control protocol, the IEEE 1394 AV/C protocol, IEC 61883 protocol, or their modifications may be used. As will be described below, in this embodiment, there is no concept of isochronous channel on the radio LAN but a field called source ID (SID) is provided in data to be transferred such that each node that is transmitting QOS data to the radio section can uniquely identify the QOS data that is being transferred, and this SID value can be used for the judgement of the data flow, as in the isochronous channel of the IEEE 1394. FIG. 39 shows an exemplary format of this radio node control packet. The source of this packet is the relay node 2102.
[0197] The radio node 2103 that received this packet recognizes that data will be transferred with QOS by having SID value of [alpha] attached thereto.
[0198] After that, the transmission node 2101 transfers the encrypted MPEG video through the isochronous channel #x (steps S2603, S2506). The contents key is assumed to be K1. This encryption key is derived as a function of the exchange key or seed to be described below.
[0199] Also, the frame for transmitting this encrypted MPEG video may contain "transmission node ID" for identifying the transmission node, besides the isochronous channel number.
[0200] The relay node 2102 that received these data recognizes that data are encrypted, refers to the "transmission node ID" contained in the received data for example, recognizes that this data is transmitted by the transmission node 2101 (step S2709), and carries out the authentication target query with respect to the transmission node 2101 in order to ascertain "which sub-unit of the transmission node 2101 is transmitting these data through the isochronous channel #x" (step S2507, S2710). At this point, the isochronous channel number (#x) through which data are transferred is described therein so that the transmission node 2101 can identify the sub-unit that is transmitting data, and the own sub-unit that received these data (the sub-unit ID=0 of the MPEG decoding/display sub-unit of the relay node 2102 in this embodiment) is also notified. This plays the role of notifying the authentication target as seen from the transmission node 2101.
[0201] Note that this authentication target query packet and the authentication target reply packet to be described below may have data encrypted or hashed by the private key of the authentication organization as an electronic signature, so as to be able to confirm the absence of alteration, etc.
[0202] Now, the transmission node 2101 that received the authentication target query (step S2604) recognizes that the sub-unit that is receiving data transmitted to the isochronous channel #X is the MPEG decoding/display sub-unit of the relay node 2102, and notifies that the sub-unit that is transmitting data to the isochronous channel #x is the video transmission sub-unit (sub-unit ID=0), to the relay node 2102 as the authentication target reply packet (step S2508, S2605).
[0203] In this way, the relay node 2102 can recognize that the sub-unit that is transmitting data to the isochronous channel #x is the video transmission sub-unit (sub-unit ID=0) of the transmission node 2101 (step S2711).
[0204] The (MPEG decoding/display sub-unit proxy function of the) relay node 2102 that recognized that the sub-unit that is transmitting data to the isochronous channel #x is the video transmission sub-unit of the transmission node 2101 then carries out the authentication request with respect to the video transmission sub-unit of the transmission node 2101. This authentication request is transferred along with the authentication format (device certificate) (Bcert) of the relay node or the MPEG decoding/display sub-unit of the relay node (steps S2509, S2606, S2607, S2712). This exchange of the authentication request and the authentication format (device certificate) is also carried out from (the video transmission sub-unit of) the transmission node 2101 with respect to (the MPEG decoding/display sub-unit of) the relay node 2102, similarly as in the first embodiment (steps S2510, S2608, S2713, S2714). The information regarding the sub-unit is also exchanged at the authentication and key exchange in this second embodiment so that the key to be used can be made different even for communications between the same devices when the sub-unit that is carrying out communication is different.
[0205] After completing the mutual authentication, these two nodes carry out the authentication and key exchange procedure similarly as in the first embodiment (steps S25111, S25112, S2609, S2715) so as to share the authentication key Kauth1. Using this authentication key, the transmission node 2101 carries out the transfer of the exchange key or seed to the relay node 2102 (steps S2512, S2610, S2716), so that it becomes possible for the relay node 2102 to ascertain the value of the contents key K1 (step S2717).
[0206] The MPEG video encrypted by using the contents key K1 that is transferred thereafter (via the isochronous channel #x) (steps S2513, S2611, S2612) is decrypted at the relay node 2102 (steps S2514, S2718), re-encrypted by using the contents key K2 that is separately provided for the radio section (steps S2515, S2516, S2719), and transmitted to the radio node 2103 in a form that guarantees QOS on the radio section (steps S2517, S2720, S2803). At this point, the MPEG video passes through a path of the ISO signal transmission and reception unit 2203, the decryption unit 2204, the encryption unit 2205, and the

radio ISO signal transmission and reception unit 2206.
[0207] As described above, data may be transmitted by attaching a value unique at the relay node 2102 called source ID such that the relay node 2102 can identify data that is being transmitted to the radio section side at this point. Here, this unique value is assumed to be [alpha]. Namely, the data with the value [alpha] attached are data received from the isochronous channel #x of the IEEE 1394 (that are decrypted by using the contents key K1 and re-encrypted by using the contents key K2). The relay node 2102 is recognizing that data that are transmitted to the radio section by attaching the SID value [alpha] are data transmitted from the proxy function of the video transmission sub-unit on the radio section side of the own device.
[0208] The operation of the radio node 2103 that received these data are basically the same as the operation of the relay node 2102 that received the encrypted data as described above.
[0209] Namely, the radio node 2103 that received these data recognizes that data are encrypted, refers to the "source address" contained in the received data for example, recognizes that this data is transmitted by the relay node 2102, and carries out the authentication target query with respect to the relay node 2102 in order to ascertain "which sub-unit of the relay node 2102 is transmitting these data by attaching the value [alpha] thereto" (step S2518, S2804).
[0210] At this point, the SID value ([alpha]) with which data are transferred is described therein so that the relay node 2102 can identify the sub-unit that is transmitting data, and the receiving side sub-unit that received these data (the sub-unit ID=0 of the MPEG decoding/display sub-unit of the radio node 2103 in this embodiment) is also notified. This plays the role of notifying the authentication target as seen from the relay node 2102.
[0211] The relay node 2102 that received the authentication target query (step S2721) recognizes that the sub-unit that is receiving data transmitted with the SID=[alpha] is the MPEG decoding/display sub-unit of the radio node 2103, and notifies that the sub-unit that is transmitting data by attaching the SID=[alpha] thereto is the video transmission sub-unit, to the radio node 2103 as the authentication target reply packet (step S2519, S2722, S2805).
[0212] In this way, the radio node 2103 can recognize that the sub-unit that is transmitting data by attaching the SID=[alpha] thereto is the video transmission sub-unit of the relay node 2102.
[0213] The (MPEG decoding/display sub-unit of the) radio node 2103 that recognized that the sub-unit that is transmitting data by attaching the SID=[alpha] thereto is the video transmission sub-unit of the relay node 2102 then carries out the authentication request with respect to the video transmission sub-unit of the relay node 2102 (steps S2520, S2723, S2724, S2806). This authentication request is transferred along with the authentication format (device certificate) (Dcert) of the radio node (or the MPEG decoding/display sub-unit of the radio node). This exchange of the authentication request and the authentication format (device certificate) is also carried out from (the video transmission sub-unit of) the relay node 2102 with respect to (the MPEG decoding/display sub-unit of) the radio node 2103 (steps S2521, S2725, S2807).
[0214] After completing the mutual authentication, these two nodes carry out the authentication and key exchange procedure (steps S2522, S2523, S2726, S2808) so as to share the authentication key Kauth2. Using this authentication key, the relay node 2102 carries out the transfer of the exchange key or seed to the radio node 2103 (steps S2524, S2727, S2809), so that it becomes possible for the radio node 2103 to ascertain the value of the contents key K2 (step S2810).
[0215] Note that, in the above description, the authentication and key exchange between the transmission node and the relay node, and the authentication and key exchange between the relay node and the radio node are carried out sequentially in this order, but their order may be reserved, or both of them may be carried out in parallel.
[0216] The MPEG video encrypted by using the contents key K1 that is transferred thereafter (steps S2525) is decrypted at the relay node 2102 (steps S2526), re-encrypted by using the contents key K2 that is separately provided for the radio section (steps S2527, S2528, S2728), and transmitted to the radio node 2103 in forms of radio frames to which the SID=[alpha] is attached (steps S2529, S2729).
[0217] This time, the radio node 2103 can calculate the content key K2 using the exchange key or seed acquired earlier, so that the received data are decrypted (steps S2530, S2811), and playbacked at the display unit 2307 (step S2812).
[0218] In this way, even in the interconnected environment where the proxy node exists between the 1394 bus and the radio network, it is possible to carry out the transfer of data that require the contents protection such as the actual MPEG video, etc., in such a way that data are encrypted throughout the entire route so that the copying is impossible and therefore the safe data transfer is possible, as the authentication procedure and the key exchange procedure are carried out by the relay node and the transmission node, and by the relay node and the reception node, at their respective sections. As a result, it becomes possible to carry out the data transfer that accounts for the copy protection even in such an interconnected environment.
[0219] Of course, there is a possibility of data copying at a portion where "raw MPEG data" flows in the relay node 2102, or more specifically between the decryption unit 2204 and the encryption unit 2205, so that it is advantageous to provide a measure against the data copying at this portion (such as forming the decryption unit and the encryption unit as a single LSI, for example) so that the eavesdropping of data (illegal copying) by attaching a probe to this portion becomes practically impossible.

Third Embodiment
[0220] Referring now to FIG. 40 to FIG. 54, the third embodiment of a relay device and a communication device according to the present invention will be described in detail.
[0221] FIG. 40 shows an exemplary overall configuration of networks In this embodiment. As shown in FIG. 40, in this third embodiment, an IEEE 1394 bus 6104 which is a home network of some home and a public network (which is assumed to be the Internet here as an example but may be a telephone network, etc.) 6105 are connected by a home gateway 61-2, and the exchange of data such as video data is to be carried out between a transmission node 6101 and a reception node 6103 after carrying out the authentication procedure and the encryption procedure. Here, it is assumed that (an access network portion of) the Internet 6105 has a very narrow communication bandwidth compared with the IEEE 1394 bus 6104 so that the video data (which are assumed to be MPEG2 video data as an example) exchanged on the IEEE 1394 bus cannot be transmitted directly because of the lack of bandwidth, and for this reason the transmission is to be carried out after applying the transcoding, that is, the code conversion from MPEG2 codes to MPEG4 codes, at the home gateway 6102.
[0222] In this third embodiment, similarly as in the second embodiment, the series of copy protection procedure, that is the authentication procedure and the encrypted data exchange, is terminated at the home gateway. Namely, each copy protection procedure is closed between the transmission node and the home gateway, and between the home gateway and the reception node. In this embodiment, the home gateway also provides the proxy services with respect to the transmission node or the reception node, but for the

copy protection, the home gateway itself has the authentication format (device certificate) and the home gateway itself terminates a responsibility for the encrypted MPEG data transfer in the 1394 bus section and the radio section.
[0223] FIG. 41 shows an exemplary internal configuration of the transmission node 6101, which is basically the same as in the above embodiments.
[0224] FIG. 42 shows an exemplary internal configuration of the home gateway 6102. The basic configuration of the home gateway 6102 is the similar to that of the relay node of the second embodiment except that it has an Internet interface 6202 instead of the radio interface, a proxy home page creation unit 6210 instead of the proxy sub-unit configuration unit, a home page creation and storage unit 6211, and an MPEG2/MPEG4 conversion unit 6214 between the decryption unit 6204 and the encryption unit 6205. Each of these differences will be described in detail below.
[0225] The home gateway 6102 has a function for providing functions of a node on the IEEE 1394 bus side as a proxy server of a node on the IEEE 1394 bus side (the transmission node 6101 in this embodiment) with respect to a node on the Internet side. The service provided by the transmission node 6101 (the video transmission service in this embodiment) is accessible through a home page provided by the home gateway 6102. Here, from a viewpoint of the reception node 6103, the service of the transmission node 6101 appears through the home page of the home gateway 6102 so that it may be interpreted as the service on the IP (Internet) that is provided by the home gateway 6102.
[0226] Also, similarly as in the second embodiment, the home gateway 6102 has a function for forwarding data (MPEG2 video data) received from the IEEE 1394 bus side to the Internet side, but the procedure related to the copy protection such as authentication and data encryption, etc., is terminated at the home gateway 6102 both in the IEEE 1394 bus section and in the Internet section. An IEEE 1394 copy protection processing unit 6208 has the authentication format (device certificate) Bcert for the IEEE 1394 bus side, while an Internet side copy protection processing unit 6212 has the authentication format (device certificate) Ccert for the Internet section side, and the encrypted data entered from the isochronous channel of the IEEE 1394 bus are processed by the sequence of reception at the ISO signal transmission reception unit 6203->decryption at the decryption unit 6204->transcoding of the decrypted MPEG2 video to MPEG4 video at the MPEG2/MPEG4 conversion unit 6214->re-encryption of the MPEG4 video at the encryption unit 6205->transmission to the Internet side at the AV signal transmission and reception unit 6206.
[0227] Here, it is assumed that Acert and Bcert are the authentication formats (device certificates) that were issued by the same authentication organization (the authentication organization responsible for the IEEE 1394 copy protection), but the authentication formats (device certificates) of the Internet section (Ccert and Dcert to be described below) may or may not be issued by the same authentication organization, so that the authentication formats (device certificates) issued by a different authentication organization that is responsible for the Internet section may be used.
[0228] Note that, in this embodiment, the authentication formats (device certificates) (Acert, Bcert, Ccert, Dcert) are provided one for each sub-unit (each sub-unit type) or one for each Internet application, rather than one for each node (or network interface). Namely, different authentication formats (device certificates) may be used by different Internet applications. Here, the flow indicates a series of data flow that is expressed by the set of (source address, source port. destination address, destination port) of the Internet.
[0229] Next, FIG. 43 shows an exemplary internal configuration of the reception node 6103, in which a copy protection processing unit 6303 has the authentication format (device certificate) Dcert for the Internet, and which differs from the second embodiment in that interfaces (an Internet interface 6301, a control packet transmission and reception unit 6302, an AV signal transmission and reception unit 6304) are compatible with the Internet. Here, the control packet transmission and reception unit 6302 may be a packet transmission and reception module having TCP transport protocol while the AV signal transmission and reception unit 6394 may be a packet transmission and reception module having UDP transport protocol.
[0230] Next, the actual operation sequence for the entire MPEG video transmission after applying the copy protection will be described with references to an exemplary overall sequence shown in FIGS. 44 and 45, an exemplary flow chart for the transmission node 6101 shown in FIGS. 46 and 47, an exemplary flow chart for the home gateway 6102 shown in FIGS. 48, 49, 50 and 51, and an exemplary flow chart for the reception node 6103 shown in FIGS. 52 and 53.
[0231] First, the home gateway 6102 collects the attribute and the configuration information of the transmission node 6101, by reading the IEEE 1212 register of the transmission node 6101, for example (steps S6501, S6601, S6701, S6502, S6602, S6702). Through this, the home gateway 6102 comprehends that the transmission node 6101 has the video transmission function, the panel function, and the authentication format (device certificate).
[0232] On a basis of this, the home gateway 6102 creates a home page for the remote controlling of the transmission node 6101 (step S6503). Basically, a display screen similar to the control panel possessed by the transmission node 6101 is created as "home page for transmission node control". Control buttons and the like that are arranged on the home page are set in correspondence to buttons of the panel sub-unit of the transmission node 6101 and a list of correspondences is described in a conversion table inside the proxy home page creation unit 6210. For example, when there is a button with a description of "playback" in the panel sub-unit of the transmission node 6101, a button with a description of "playback" is provided in the home page as well, and this relationship is described in the above mentioned conversion table. If a user of this home page presses this button, an interaction indicating that "the button is pressed" with respect to the "playback" button of the panel sub-unit of the transmission node 6101 will be returned from the home gateway 6102. A part (a) of FIG. 54 shows an exemplary form of a panel possessed by the panel sub-unit of the transmission node 6101, and a part (b) of FIG. 54 shows an exemplary form of a corresponding home page for transmission node control created by the home gateway 6102.
[0233] Now, when the reception node 6103 on the Internet accesses the home gateway 6102 through the Internet and requests a home page containing a control display screen for the transmission node 6101, this home page is sent to the reception node 6103 (steps S6504, S6801, S6703). Upon viewing this home page, suppose that a user of the reception node 6103 pressed a button for requesting the video transmission on the display screen (such as the "playback" button shown in a part (b) of FIG. 54, for example). As a result, an interaction indicating that "the playback button is pressed", for example, is notified to the home gateway 6102 via the Internet using HTTP (steps S6505, S6802, S6704).
[0234] Before or after this notification, the determination of the IP flow by which the stream to be exchanged is to be transferred, that is the set of (source IP address, source port, destination IP address, destination port), the negotiation of the session control (coding scheme, authentication scheme), etc., are carried out between the home gateway 6102 and the reception node 6103 (steps S6505, S6705, S6803). For example, the coding scheme, the authentication scheme, and the port number are determined using RTSP (Realtime Transport Streaming Protocol), SDP (Session Description Protocol), etc.
[0235] On a basis of these processings, the home gateway 6102 recognizes that the substance that carries out the video transmission is the video transmission sub-unit of the transmission node 6101, and issues

commands for setting up an isochronous channel #x to be used for the data transfer and for requesting the video transmission to the video transmission sub-unit, using the AV/C protocol, etc., with respect to the transmission node 6101 (step S6506).
[0236] In response, the encrypted MPEG video is transmitted from the transmission node 6101 through the isochronous channel #x to the home gateway 6102 (steps S6507, S6603, S6604). After that, the authentication target query/reply, the authentication request, the authentication and key exchange procedure, the exchange key/seed transfer, etc., are carried out by the procedure similar to that of the IEEE 1394 side of the second embodiment, such that it becomes possible for the home gateway 6102 to calculate the contents key K1 (steps S6508 to S6514, S6605 to S6611, S6706 to S6715).
[0237] Thereafter, the home gateway 6102 receives the encrypted MPEG video through the isochronous channel #x (steps S6515, S6612, S6613), and decrypts it into MPEG2 video by using the contents key K1 at the decryption unit 6204 (steps S6516, S6517, S6716). Next, the extracted MPEG2 video is transcoded into MPEG4 video at the MPEG2/MPEG4 conversion unit 6214 (step S6518). This MPEG4 video is re-encrypted by using the contents key K2 at the encryption unit 6205 (steps S6519, S6520, S6717, S6718), and converted into IP packets. In this case, IP packets in which the source IP address is C (IP address of the home gateway), the source port number is c, the destination IP address is D (IP address of the reception node) and the destination port number is d as determined by the earlier session control procedure are generated (steps S6521, S6719).
[0238] Upon receiving these IP packets, the reception node 6103 recognizes that the received data are encrypted (step S6804). The reception node 6103 recognizes that the home gateway 6102 is transmitting these data by referring to the IP header of the arrived packets, for example, and transmits the authentication request to the home gateway 6102 (steps S6522, S6805). This authentication request packet may also be an IP packet. As the port number for the authentication request, a number allocated to the procedure for carrying out the authentication in advance may be used. At this point, the authentication request packet is transferred by attaching the flow ID (C, c, D, d) of the stream transfer. As a result, the home gateway 6102 can recognize the flow to which the authentication request is directed. Although not shown in the figure, this authentication request also contains the authentication format (device certificate) (for this stream) of the reception node, etc. Also, the fact that RTP (Realtime Transport Protocol) is used as the transport protocol, etc., may also be notified at the same time.
[0239] Upon receiving this authentication request, the home gateway 6102 recognizes that it is the authentication request for the flow (C, c, D, d), and returns the authentication request containing the authentication format (device certificate) for this flow, to the reception node (steps S6523, S6720 to S6722, S6806, S6807). At this point, this authentication request contains the above described flow ID, etc.
[0240] Next, these two nodes carries out the authentication and key exchange procedure, the exchange key/seed transfer, etc., using IP packets (steps S6524 to S6526, S6723, S6724, S6808 to S6810). As a result, it becomes possible for the reception node 6103 to generate the contents key K2.
[0241] Thereafter, when the MPEG4 data that are encrypted by using the contents key K2 are transmitted through the flow (C, c, D, d) (steps S6527 to S6533, S6725, S6726, S6811), these data can be decrypted by using the contents key K2 that is prepared as described above (step S6534). The decrypted MPEG4 data are decoded at the MPEG decoding unit 6306 (step S6812) and playbacked at the display unit 6307 (step S6813).
[0242] In this way, even in the environment where the home network and the Internet are interconnected, it is possible to carry out the transfer of data that require the contents protection such as the actual MPEG video, etc., in such a way that data are encrypted throughout the entire route so that the copying is impossible and therefore the safe data transfer is possible, as the authentication procedure and the key exchange procedure are carried out by the home gateway and the transmission node, and by the home gateway and the reception node. As a result, it becomes possible to carry out the data transfer that accounts for the copy protection even in such an interconnected environment.
[0243] Similarly as in the second embodiment, there is a possibility of data copying at a portion where "raw MPEG data" flows in the home gateway 6102, or more specifically between the decryption unit 6204, the MPEG2/MPEG4 conversion unit 6214, and the encryption unit 6205, so that it is possible to provide a measure against the data copying at this portion, such as sealing this portion within a single LSI, for example.

Fourth Embodiment
[0244] Referring now to FIG. 55 to FIG. 64, the fourth embodiment of a relay device and a communication device according to the present invention will be described in detail.
[0245] In the first embodiment, the authentication and key exchange scheme in the case where the relay node is connected to both the IEEE-1394 bus and the radio network and the encrypted video data are to be exchanged between the transmission node on the IEEE 1394 bus and the radio node on the radio network has been described. In the first embodiment, the actual authentication and key exchange as represented by the exchange of the authentication format (device certificate), etc., is directly carried out between the transmission node and the radio node, and the relay node is provided in a form of transparently relaying these data.
[0246] In contrast, in this fourth embodiment, the authentication and key exchange is carried out separately between the transmission node and the relay node and between the relay node and the radio node, as in the second embodiment. Here, however, unlike the second embodiment, this fourth embodiment uses a scheme in which the decryption and the re-encryption of the contents data at the relay node are unnecessary. Namely, the second embodiment employs a procedure in which the encryption in the IEEE 1394 section of the arrived data is decrypted and then re-encrypted for the radio section at the relay node, whereas this fourth embodiment employs a scheme in which the encrypted data arrived from the IEEE 1394 bus side can be transferred directly to the radio network.
[0247] FIG. 55 shows an exemplary overall configuration of a home network at some home, which is basically the same as in the second embodiment.
[0248] FIG. 56 shows an exemplary internal configuration of the transmission node 9101, which is also basically the same as in the second embodiment. The authentication format (device certificate) Acert is provided one for each node.
[0249] FIG. 57 shows an exemplary internal configuration of the relay node 9102. The authentication formats (device certificates) Bcert and Ccert are provided one for each network interface (Bcert for the IEEE 1394 side and Ccert for the radio network side). This relay node 9102 is similar to that of the second embodiment except that the encrypted stream signals are directly exchanged between the ISO signal transmission and reception unit 9203 on the IEEE 1394 side and the radio ISO signal transmission and reception unit 9206 on the radio network side (without going through the process of decryption/re-encryption).
[0250] FIG. 58 shows an exemplary internal configuration of the radio node 9103, which is also basically the

same as that of the second embodiment. The authentication format (device certificate) Dcert is provided one for each node.
[0251] As in the previous embodiments, the relay node 9102 has proxy service functions for services on the radio network with respect to the IEEE 1394 side and services on the IEEE 1394 with respect to the radio network side, but the details of these functions will be omitted here.
[0252] Next, FIG. 59 shows an exemplary overall sequence of this embodiment. Similarly as in the previous embodiments, the relay node is advertising the service (video transmission sub-unit) provided by the transmission node as a proxy to the radio network side, and when (the video decoding sub-unit of) the radio node requests the service (MPEG video transfer request) with respect to the proxy function of the relay node, the relay node makes the actual video transfer request with respect to the video transmission sub-unit of the transmission node that is providing the actual service. It is assumed that the actual video data are to be transferred in an encrypted form, through the isochronous channel #x on the IEEE 1394 and through the radio isochronous channel #y on the radio network. The details are the same as in the previous embodiments so that the detailed description will be omitted here.
[0253] FIG. 60 shows an exemplary operation procedure of the transmission node 9101, FIGS. 61 and 62 show an exemplary operation procedure of the relay node 9102, and FIGS. 63 and 64 show an exemplary operation procedure of the radio node 9103.
[0254] In this embodiment, the procedure basically follows the authentication and key exchange scheme called "5C Digital Transmission Content Protection Specification" which is the copyright protection scheme on the IEEE 1394. Note that this embodiment is directed to the case of carrying out the authentication and key exchange in units of nodes (the case of carrying it out in units of sub-units will be described in the fifth embodiment).
[0255] Now, the transmission node 9101 transfers the MPEG video that is encrypted by using the contents key K on the isochronous channel #x of the IEEE 1394 (steps S8501, S8601, S8701). The relay node 9102 that received this MPEG video transfers this MPEG video directly (leaving the received MPEG video in a form encrypted by using the contents key K) to the radio isochronous channel #y on the radio network side (steps S8509, S8701).
[0256] The relay node 9102 that recognized that data received through the isochronous channel #x are encrypted then recognizes that there is a need to carry out the authentication and key exchange with the transmission node 9101 by referring to the transmission node ID field (SID field) of the CIP header of the arrived data, for example (step S8801), and transfers the authentication request packet containing the authentication format (device certificate) Bcert, to the transmission node 9101 (steps S8502, S8702).
[0257] The transmission node 9101 that received this packet then transmits the authentication request packet containing the authentication format (device certificate) Acert of the transmission node, to the relay node 9102 (Steps S8503, S8602, S8603, S8703).
[0258] Next, the authentication and key exchange procedure is carried out such that the authentication key Kauth1 is secretly shared between the transmission node 9101 and the relay node 9102 (steps S8504, S8505, S8604, S8704).
[0259] In the IEEE 1394 copyright protection scheme, the contents key K is calculated by a function J with three variables including the exchange key Kx, the seed Nc, and the encryption control information EMI. Namely, K=J(Kx, Nc, EMI). Here, the EMI is a value that is always attached to the encrypted data to be transferred. Consequently, there is also a need for the transmission node 9101 to notify values of the exchange key Kx and the seed Nc to the receiving side (the relay node, as well as the radio node in the case of this embodiment).
[0260] For this reason, the transmission node 9101 transmits this information to the relay node 9102, in a form of f(Kx, Kauth1) using the authentication key Kauth1 that is shared with the relay node 9102 and the known function f (steps S8506, S8605, S8708, S8709). The relay node 9102 can calculate the value of Kx from this value. Similarly, the value of the seed Nc is transferred from the transmission node 9101 to the relay node 9102 (steps S8507, S8606, S8710). At this point, the relay node 9102 has recognized the values of Kx and Nc that are necessary in generating the contents key K for decryption.
[0261] Now, the similar procedure is also carried out between the relay node 9102 and the radio node 9103 (steps S8510 to S8513, S8705 to S8707, S8802 to S8804). This procedure is similar to the authentication and key exchange procedure between the transmission node 9101 and the relay node 9102 so that the details will be omitted here. Note here that encrypted data to be transferred on the radio isochronous channel #y of the radio network may also be attached with address information, etc., by which the relay node 9102 that is the source node can be identified.
[0262] Now, suppose that the authentication key Kauth2 is shared between the relay node 9102 and the radio node 9103. In this embodiment, the relay node 9102 forwards the encrypted MPEG video directly to (the radio isochronous channel #y of) the radio network without decrypting it, so that there is a need for the relay node 9102 to notify the values of the exchange key Kx and the seed Nc that are the same as in the IEEE 1394 section, to the radio node 9103. (Conversely, if this can be notified, it becomes possible for the radio node 9103 to carry out the decryption. Here, it is assumed that the IEEE 1394 section and the radio network section are operated by the same contents protection policy.) Consequently, the relay node 9102 transmits the respective values of Kx and Nc that are calculated from data received at the steps S8506 and S8507, to the radio node 9103 similarly (steps S8514, S8515, S8709, S8711, S8805 to S8807). More specifically, the value of Kx is transmitted to the radio node 9103 by calculating f(Kx, Kauth2) using the value of the authentication key Kauth2, while the value of Nc is transferred as it is.
[0263] The radio node 9103 can recognize the values of Kx and Nc by using the same procedure as the relay node in this way, so that it becomes possible for the radio node 9103 to calculate the value of the contents key K using the similar function J (step S8516).
[0264] Thus, when the MPEG video that is encrypted by using the contents key K and transmitted from the transmission node 9101 is transferred up to the radio node 9103 as the relay node 9102 forwards it directly without carrying out the decryption (steps S8508, S8517, S8607, S8712, S8809), it can be decrypted by using the value of the contents key K that is calculated at the earlier step S8516 (steps S8518, S8810). Then, decoding, displaying, etc., of the MPEG video are carried out.
[0265] Note that this embodiment has been described by assuming that the radio isochronous channel is defined on the radio network and the encrypted MPEG video is transferred on this radio isochronous channel, but the similar scheme for forwarding the values of Kx and Nc from the relay node to the radio node is also applicable to the case where the QOS data transfer on the radio network transfers radio frames similar to the Ethernet as in the second embodiment.
[0266] In other words, the decryption and the re-encryption at the relay node 9102 can be made unnecessary by the scheme of this embodiment, so that the fast packet transfer becomes possible and therefore the low cost relay node can be realized.
[0267] Note that, in this case, even if there is another node other than the transmission node 9101 on the IEEE 1394 side, it is impossible to transmit the encrypted data (data having the same EMI, to be precise)

that are encrypted by using another contents key from that another node to the radio node 9103 via the relay node 9102. In the mechanism adopted here, the contents key is basically to be determined by the transmission node 9101 of data so that there is a high probability for that another node to select another contents key. However, the contents key K is already uniquely defined between the relay node 9102 and the radio node 9103. That is, only one contents key can be shared for the same EMI value between the relay node 9102 and the radio node 9103. Consequently, at most one contents key can be used between these two nodes so that even if data (encrypted by using another contents key) from another node are received, another contents key cannot be generated at a time of transferring data from the relay node 9102 to the radio node 9103 so that data cannot be decrypted.
[0268] Thus, in the case where there is a transmission request for the encrypted data that requires the use of another contents key with respect to a node (the radio node 9103 in the case of this embodiment) that is already transmitting encrypted data (the case where there is a service request with respect to the proxy service for another node of the IEEE 1394, for example), the above noted contradiction can be prevented if the relay node 9102 refuses such a request. The similar effect can also be achieved if the relay node 9102conceals the other services (sub-units) to the radio node 9103 (by interrupting the proxy service providing itself, or by interrupting the proxy service that is associated with the encrypted stream transfer, etc.) in the case where the encrypted data transmission with respect to the radio node 9103 is already taking place.

Fifth Embodiment
[0269] Referring now to FIG. 65 to FIG. 68, the fifth embodiment of a relay device and a communication device according to the present invention will be described in detail.
[0270] The fourth embodiment is directed to the scheme in which the authentication and key exchange is carried out separately between the transmission node and the relay node and between the relay node and the radio node, and there is no need to carry out the decryption and the re-encryption at the relay node.
[0271] In contrast, this fifth embodiment is directed to the scheme in which there is also no need to carry out the decryption and the re-encryption at the relay node, but the authentication and key exchange on the radio network side can be carried out in units of sub-units as in the second embodiment, so that a plurality of contents keys can be used between the same two nodes. According to this embodiment, the simultaneous reception of the encrypted data from a plurality of transmission nodes on the IEEE 1394 becomes possible.
[0272] FIG. 65 shows an exemplary overall configuration of a home network at some home, which is basically similar to that of the fourth embodiment except that there are two transmission nodes (P and Q).
[0273] The internal configuration of each of the transmission nodes 9801 and 9811 is the same as in the fourth embodiment.
[0274] The internal configuration of the relay node 9802 is also similar to that of the fourth embodiment except that the authentication and key exchange is to be carried out in units of nodes on the IEEE 1394 side while the authentication and key exchange is to be carried out in units of sub-units on the radio network side.
[0275] The internal configuration of the radio node 9803 is also similar to that of the fourth embodiment except that the authentication and key exchange is to be carried out in units of sub-units.
[0276] Note that the operation procedures of the transmission nodes 9801 and 9811 and the radio node 9803 are the same as in the fourth embodiment. Also, the operation procedure of the relay node 9802 in the case of relaying with respect to a single transmission node is basically the same as in the fourth embodiment.
[0277] As in the previous embodiments, the relay node 9802 has proxy service functions for services on the radio network with respect to the IEEE 1394 side and services on the IEEE 1394 with respect to the radio network side, but the details of these functions will be omitted here.
[0278] Next, FIG. 66 shows an exemplary operation procedure of the relay node 9802 in the case of relaying with respect to plural transmission nodes, and FIGS. 67 and 68 show an exemplary overall sequence of this embodiment. Similarly as in the previous embodiments, the relay node is advertising the service (video transmission sub-unit) provided by the transmission node as a proxy to the radio network side, and when (the video decoding sub-unit of) the radio node requests the service (MPEG video transfer request) with respect to the proxy function of the relay node, the relay node makes the actual video transfer request with respect to the video transmission sub-unit of the transmission node that is providing the actual service. It is assumed that the actual video data are to be transferred in an encrypted form, through the isochronous channel #x on the IEEE 1394 and through the radio isochronous channel #y on the radio network. The details are the same as in the previous embodiments so that the detailed description will be omitted here.
[0279] In this embodiment, the procedure also basically follows the authentication and key exchange scheme called "5C Digital Transmission Content Protection Specification" which is the copyright protection scheme on the IEEE 1394.
[0280] Now, the transmission node P 9801 transfers the MPEG video that is encrypted by using the contents key K1 on the isochronous channel #x of the IEEE 1394 (steps S9201, S9301). Similarly as in the fourth embodiment, it is assumed that the contents key K1 is calculated by K1=J(Kxp, Ncp, EMI). The relay node 9802 that received this MPEG video transfers this MPEG video directly (leaving the received MPEG video in a form encrypted by using the contents key K1) to the radio isochronous channel #y on the radio network side (steps S9209, S9301).
[0281] The procedure (steps S9202 to S9207, S9302) by which the relay node 9802 makes the authentication request with respect to the transmission node P, carries out the key exchange, and obtains the exchange key Kxp and the seed Ncp is the same as in the fourth embodiment, so that the details will be omitted here. At this point, the relay node 9802 has recognized the values of Kxp and Ncp that are necessary for decryption.
[0282] Now, the similar authentication and key exchange procedure is also carried out between the relay node 9802 and the radio node 9803 (steps S9210 to S9217, S9303). This procedure is similar to the authentication and key exchange procedure between the transmission node and the relay node in the second embodiment so that the details will be omitted here. Note here that the authentication target query, the authentication target reply, or the authentication request may be made by mounting thereon a sub-unit ID, a channel number, or an identifier of a plug that will carry out transmission and reception of the encrypted data. In this way, it becomes possible for the relay node 9802 or the radio node 9803 to identify the encrypted data to which the authentication and key exchange procedure is directed, and it becomes possible to notify different keys for the encrypted data using different keys even in the authentication and key exchange between the same two nodes, as will be described below. In the case of including the channel number in the authentication request, the authentication target query of the step S9210 and the authentication target reply of the step S9211 become unnecessary.

[0283] Now, suppose that the authentication key Kauth1 is shared between the relay node 9802 and the radio node 9803. In this embodiment, the relay node 9802 also forwards the encrypted MPEG video directly to (the radio isochronous channel #y of) the radio network without decrypting it, so that there is a need for the relay node 9802 to notify the values of the exchange key Kxp and the seed Ncp, to the radio node 9803. (Conversely, if this can be notified, it becomes possible for the radio node 9803 to carry out the decryption.) Consequently, the relay node 9802 transmits the respective values of Kxp and Ncp that are calculated from data received at the steps S9206 and S9207, to the radio node 9803 similarly (steps S9216, S9217). More specifically, the value of Kxp is transmitted to the radio node 9803 by calculating f(Kxp, Kauth1) using the value of the authentication key Kauth1 (step S9216).
[0284] The radio node 9803 can recognize the values of Kxp and Ncp by using the same procedure as the relay node 9802 in this way, so that it becomes possible for the radio node 9803 to calculate the value of the contents key K1 using the similar function J (step S9218).
[0285] Thus, when the MPEG video that is encrypted by using the contents key K1 and transmitted from the transmission node P 9801 is transferred up to the radio node 9803 as the relay node 9802 forwards it directly without carrying out the decryption (steps S9208, S9219), it can be decrypted by using the value of the contents key K1 that is calculated at the earlier step S9218 (steps S9220). Then, decoding, displaying, etc., of the MPEG video are carried out.
[0286] By the scheme of this embodiment, the decryption and the re-encryption at the relay node 9802 also can be made unnecessary by the scheme of this embodiment, so that the fast packet transfer becomes possible and therefore the low cost relay node can be realized.
[0287] Now, the case where another transmission node Q 9811 transmits data encrypted by using another contents key K2 with respect to the radio node 9803 via the relay node 9802 at the same time (steps S9221, S9229, S9304) will be considered.
[0288] Similarly as in the first half of this embodiment, the authentication and key exchange is carried out between the transmission node Q 9811 and the relay node 9802 (steps S9222 to S9227) so that the relay node 9802 can obtain the respective values of the exchange key Kxq and the seed Ncq.
[0289] In this embodiment, the authentication between the relay node 9802 and the radio node 9803 is to be carried out in units of sub-units, so that if transmission and reception of the encrypted data are carried out between different sub-units, a plurality of authentication and key exchange procedures can be carried out between the relay node 9802 and the radio node 9803.
[0290] Namely, similarly as in the first half of this embodiment, the authentication and key exchange is carried out between sub-units that are different from those of the first half of this embodiment (steps S9230 to S9235, S9305). Then, the relay node 9802 forwards the exchange key Kxq and the seed Ncq between the transmission node Q 9811 and the own node (relay node 9802), to the radio node 9803 (steps S9236, S9237, S9305, S9306).
[0291] The radio node 9803 can recognize the values of Kxq and Ncq in this way, so that it becomes possible for the radio node 9803 to calculate the value of the contents key K2 using the similar function J (step S9238).
[0292] Thus, when the MPEG video that is encrypted by using the contents key K2 and transmitted from the transmission node Q 9811 is transferred up to the radio node 9803 as the relay node 9802 forwards it directly without carrying out the decryption (steps S9228, S9229), it can be decrypted by using the value of the contents key K2 that is calculated at the earlier step S9238 (steps S9240). In other words, the simultaneous reception of the MPEG video data that are encrypted by using two different contents keys (K1 and K2 in this embodiment) becomes possible.
[0293] Note that the fourth and fifth embodiments have been described for an exemplary case of interconnecting the IEEE 1394 and the radio network, but the schemes of these embodiments are also applicable to the other network such as Internet.
[0294] Note also that the authentication and key exchange was carried out between certain sub-units in this embodiment, but it is possible to carry out the authentication and key exchange between certain plugs.
[0295] As described, according to the present invention, it becomes possible to carry out the contents protection procedure for transmission and reception of contents to be protected, between devices that are not connected to the same networks.
[0296] Note that the present invention is equally applicable to the case of data transfer in the direction opposite to that described in the first to fifth embodiments (the case of data transfer from the radio node to a node on the IEEE 1394, for example).
[0297] Note also that the first to fifth embodiments have been described by focusing on only one of the contents transmission function and the contents reception function in the radio node or the node on the IEEE 1394, but the radio node and the node on the IEEE 1394 can be equipped with both of the contents transmission function and the contents reception function.
[0298] Note also that the authentication procedure and the key exchange procedure (the contents key sharing procedure) are not necessarily limited to those described above, and the present invention is also applicable to the cases using various other methods.
[0299] Note also that the above embodiments have been described for the home network, but the present invention is also applicable to networks other than the home network.
[0300] It is also to be noted that the above described embodiments according to the present invention may be conveniently implemented using a conventional general purpose digital computer programmed according to the teachings of the present specification, as will be apparent to those skilled in the computer art. Appropriate software coding can readily be prepared by skilled programmers based on the teachings of the present disclosure, as will be apparent to those skilled in the software art.
[0301] In particular, each of the relay device and the communication device of the above described embodiments can be conveniently implemented in a form of a software package.
[0302] Such a software package can be a computer program product which employs a storage medium including stored computer code which is used to program a computer to perform the disclosed function and process of the present invention. The storage medium may include, but is not limited to, any type of conventional floppy disks, optical disks, CD-ROMs, magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, or any other suitable media for storing electronic instructions.
[0303] It is also to be noted that, besides those already mentioned above, many modifications and variations of the above embodiments may be made without departing from the novel and advantageous features of the present invention. Accordingly, all such modifications and variations are intended to be included within the scope of the appended claims.

REPEATER AND COMMUNICATION EQUIPMENT

Claims of corresponding document: **US 7218643 (B1)**

What is claimed is:

1. A relay device, comprising:
a first interface unit connected to a first network operated by a first protocol;
a second interface unit connected to a second network operated by a second protocol that is different from the first protocol;
a proxy configuration unit for disclosing a device/service/sub-unit on the second network as an own device/service/sub-unit provided on the relay device with respect to a first network side;
a control command reception unit for receiving control command signals destined to the own device/service/sub-unit from the first network side;
a control command transmission unit for transmitting signals corresponding to the control command signals received by the control command reception unit, to the device/service/sub-unit on the second network;
a contents protection information reception unit for receiving contents protection information destined to the own device/service/sub-unit, from a device on the first network; and
a contents protection information transfer unit for transferring the contents protection information received by the contents protection information reception unit to the device/service/sub-unit on the second network, so as to selectively relay the contents protection information transparently without making any change in the contents protection information;
wherein the contents protection information is information necessary in carrying out a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on the first network and another device/service/sub-unit on the second network.

2. A relay device, comprising:
a first interface unit connected to a first network operated by a first protocol;
a second interface unit connected to a second network operated by a second protocol that is different from the first protocol;
a proxy configuration unit for disclosing each device/service/sub-unit on the first network or the second network as an own device/service/sub-unit provided on the relay device with respect to respective another network side;
a control command reception unit for receiving control command signals destined to the own device/service/sub-unit from a side of one network to which the own device/service/sub-unit is disclosed by the proxy configuration unit;
a control command transmission unit for transmitting signals corresponding to the control command signals received by the control command reception unit, to said each device/service/sub-unit on another network different from said one network;
a contents protection information reception unit for receiving contents protection information destined to the own device/service/sub-unit from a device on the first network or the second network;
a contents protection information transfer unit for transferring the contents protection information received by the contents protection information reception unit to said each device/service/sub-unit on said another network, so as to selectively relay the contents protection information transparently without making any change in the contents protection information;
a contents reception unit for receiving contents destined to the own device/service/sub-unit and protected by a contents key obtained from the contents protection information, from a device on the first network or the second network; and
a contents transfer unit for transferring the contents received by the contents reception unit to said each device/service/sub-unit on said another network, so as to selectively relay the contents transparently without making any change in the contents;
wherein the contents protection information is information necessary in carrying out a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on the first network and another device/service/sub-unit on the second network.

3. The relay device of claim 2, further comprising:
a configuration information reception unit for receiving a configuration information from one device/service/sub-unit on the first network or the second network, the configuration information indicating at least a presence or absence of an authentication format for said one device/service/sub-unit; and
a configuration recognition unit for recognizing a configuration of said one device/service/sub-unit according to the configuration information received by the configuration information reception unit.

4. A relay device, comprising:
a first interface unit connected to a first network operated by a first protocol;
a second interface unit connected to a second network operated by a second protocol that is different from the first protocol;
a proxy configuration unit for disclosing each device/service/sub-unit on the first network or the second network as an own device/service/sub-unit provided on the relay device with respect to respective another network side;
a control command reception unit for receiving control command signals destined to the own device/service/sub-unit from a side of one network to which the own device/service/sub-unit is disclosed by the proxy configuration unit;
a control command transmission unit for transmitting signals corresponding to the control command signals received by the control command reception unit, to said each device/service/sub-unit on another network different from said one network;
a first contents protection unit for carrying out a contents protection procedure including at least an authentication and/or a key exchange, with respect to one device/service/sub-unit on the first network;
a second contents protection unit for carrying out the contents protection procedure including at least the authentication and/or the key exchange, with respect to another device/service/sub-unit on the second network, separately from the contents protection procedure carried out by the first contents protection unit;
a contents reception unit for receiving contents destined to the own device/service/sub-unit and encrypted

according to one of the first and second contents protection units; and
a contents transfer unit for transferring the contents received by the contents reception unit to said each device/service/sub-unit on said another network, by encrypting the contents according to another one of the first and second contents protection units.

5. The relay device of claim 4, wherein the first contents protection unit and the second contents protection unit use different encryption schemes or identical encryption schemes based on different keys.

6. The relay device of claim 4, wherein the contents reception unit and the contents transmission unit are sealed within a single LSI.

7. The relay device of claim 4, wherein a first key information used in the contents protection procedure in the first contents protection unit and a second key information used in the contents protection procedure in the second contents protection unit are set to be identical.

8. The relay device of claim 7, wherein the contents protection procedure in said another one of the first and second contents protection units is carried out in units of contents/services/sub-units, using a prescribed key information.

9. The relay device of claim 4, further comprising:
a configuration information reception unit for receiving a configuration information from one device/service/sub-unit on the first network or the second network, the configuration information indicating at least a presence or absence of an authentication format for said one device/service/sub-unit; and
a configuration recognition unit for recognizing a configuration of said one device/service/sub-unit according to the configuration information received by the configuration information reception unit.

10. A relay device, comprising:
a first interface unit connected to a first network operated by a first protocol;
a second interface unit connected to a second network operated by a second protocol that is different from the first protocol;
a first contents protection unit for carrying out a contents protection procedure including at least an authentication and/or a key exchange, with respect to one device/service/sub-unit on the first network;
a second contents protection unit for carrying out the contents protection procedure including at least the authentication and/or the key exchange, with respect to another device/service/sub-unit on the second network, separately from the contents protection procedure carried out by the first contents protection unit;
a contents reception unit for receiving contents destined to an own device/service/sub-unit on the relay device and encrypted according to one of the first and second contents protection units, from a device on one of the first network and the second network; and
a contents transmission unit for transmitting the contents received by the contents reception unit to a device/service/sub-unit on another one of the first network and the second network, by encrypting the contents according to another one of the first and second contents protection units;
wherein a first key information used in the contents protection procedure in the first contents protection unit and a second key information used in the contents protection procedure in the second contents protection unit are set to be identical.

11. A relay device, comprising:
a first interface unit connected to a first network operated by a first protocol;
a second interface unit connected to a second network operated by a second protocol that is different from the first protocol;
a first copy protection processing unit for carrying out a prescribed contents protection procedure including at least an authentication procedure and a key exchange procedure, with respect to one device/service/sub-unit on the first network;
a second copy protection processing unit for carrying out the prescribed contents protection procedure including at least the authentication procedure and the key exchange procedure, with respect to another device/service/sub-unit on the second network, separately from the contents protection procedure carried out by the first contents protection unit;
a contents reception unit for receiving encrypted data containing specific contents from the first interface unit;
a decryption unit for decrypting the encrypted data receiving by the contents reception unit, by using a contents protection key provided by the first copy protection processing unit, to obtain decrypted data;
a conversion unit for converting the decrypted data into converted data in another coding format;
an encryption unit for encrypting the converted data, by using a contents protection key provided by the second copy protection processing unit, to obtain re-encrypted data; and
a contents transmission unit for transferring the re-encrypted data to the second interface unit.

12. The relay device of claim 11, further comprising:
a proxy configuration unit for disclosing one device/service/sub-unit on the second network as one own device/service/sub-unit provided on the relay device with respect to a first network side, and transmitting to said one device/service/sub-unit on the second network an information having a content according to information destined to said one own device/service/sub-unit that is received from a device on the first network side, while also disclosing another device/service/sub-unit on the first network as another own device/service/sub-unit provided on the relay device with respect to a second network side, and transmitting to said another device/service/sub-unit on the first network an information having a content according to information destined to said another own device/service/sub-unit that is received from a device on the second network side;
wherein when the prescribed contents protection procedure between a device on one network among the first and second networks and a device/service/sub-unit on another network among the first and second networks is to be carried out, the proxy configuration unit carries out the prescribed contents protection procedure with the device on said one network by using one of the first and second copy protection processing units, while carrying out the prescribed contents protection procedure with the device/service/sub-unit on said another network by using another one of the first and second copy protection processing units.

13. A relay device, comprising:
a first interface unit connected to a first network operated by a first protocol;

a second interface unit connected to a second network operated by a second protocol that is different from the first protocol;
a first contents protection unit for carrying out a contents protection procedure including at least an authentication procedure and a key exchange procedure, with respect to one device/service/sub-unit on the first network;
a second contents protection unit for carrying out the contents protection procedure including at least the authentication procedure and the key exchange procedure, with respect to another device/service/sub-unit on the second network, separately from the contents protection procedure carried out by the first contents protection unit;
a contents reception unit for receiving contents destined to an own device/service/sub-unit on the relay device and encrypted according to one of the first and second contents protection units, from a device on one of the first network and the second networks; and
a contents transmission unit for transmitting the contents received by the contents reception unit to a device/service/sub-unit on another one of the first network and the second network, by encrypting the contents according to another one of the first and second contents protection units;
wherein said one of the first and second contents protection units carries out the authentication and/or the key exchange with a device/service/sub-unit on said one of the first network and the second network by referring to a relationship between the contents reception unit and the contents transmission unit, when there is a request for a procedure of the authentication and/or the key exchange with respect to said another one of the first and second contents protection units.

.....

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－174797
（P2000－174797A）
(43)公開日　平成12年６月23日(2000.6.23)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
H04L	12/46		H04L	11/00	310C
	12/28		G11B	20/10	H
G11B	20/10		H04L	9/00	673A
H04L	9/32				675D
	12/66			11/20	B

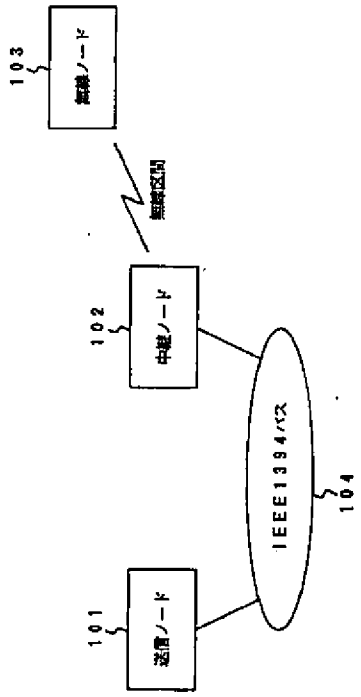
審査請求　未請求　請求項の数17　ＯＬ　（全 60 頁）　最終頁に続く

(21)出願番号　特願平11－209836
(22)出願日　平成11年７月23日(1999.7.23)
(31)優先権主張番号　特願平10－292824
(32)優先日　平成10年９月30日(1998.9.30)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　斉藤　健
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　高畠　由彰
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　中継装置及び通信装置

(57)【要約】
【課題】　同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とする中継装置を提供すること。
【解決手段】　第１のネットワーク１０４と第２のネットワークに接続され、第２のネットワーク上の装置１０３を自中継装置１０２上のものとして第１のネットワーク１０４側に開示する機能と、第１のネットワーク１０４上の装置１０１から装置１０３宛の制御コマンドを受信した場合、これに対応する制御コマンドを装置１０３へ送信する機能と、装置１０１から装置１０３宛のコンテンツ保護情報を受信した場合、これに変更を加えずに装置１０３へ送信する機能と、装置１０１から装置１０３宛に先のコンテンツ保護情報から得られるコンテンツ鍵で保護されたコンテンツを受信した場合、これに変更を加えずに装置１０３へ送信する機能とを有する。



【特許請求の範囲】

【請求項１】第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

前記第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして前記第１のネットワーク側に開示する代理構成手段と、

この装置又はサービス又はサブユニット宛の制御コマンド信号を前記第１のネットワーク側から受信する制御コマンド受信手段と、

この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を前記第２のネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、

前記第１のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、

このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記第２のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段とを具備したことを特徴とする中継装置。

【請求項２】第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

第１及び第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして各々他方のネットワーク側に開示する代理構成手段と、

この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、

この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、

前記第１又は第２のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、

このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段と、

前記第１又は第２のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛であり、前記コンテンツ保護情報から得られる

コンテンツ鍵で保護されたコンテンツを受信するコンテンツ受信手段と、

このコンテンツ受信手段で受信した前記コンテンツに変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ転送手段とを具備したことを特徴とする中継装置。

【請求項３】前記コンテンツ保護情報は、前記第１のネットワーク上の装置又はサービス又はサブユニットと、前記第２のネットワーク上の装置又はサービス又はサブユニット間の認証及び又は鍵交換を含むコンテンツ保護の手続きに関する情報であることを特徴とする請求項２に記載の中継装置。

【請求項４】第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

第１及び第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして各々他方のネットワーク側に開示する代理構成手段と、

この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、

この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、

前記第１のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第１のコンテンツ保護手段と、

前記第２のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第２のコンテンツ保護手段と、

前記第１又は第２のいずれか一方のネットワーク上の装置から、前記代理構成手段で開示した自中継装置上の装置又はサービス又はサブユニット宛であり、前記第１又は第２のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、

前記コンテンツ受信手段で受信したコンテンツを、前記第１又は第２のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第１又は第２のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備したことを特徴とする中継装置。

【請求項５】前記第１のコンテンツ保護手段と、前記第２のコンテンツ保護手段で用いられる暗号化方式は異なる方式であるか、又は異なる鍵情報に基づくものであることを特徴とする請求項４に記載の中継装置。

【請求項６】前記コンテンツ受信手段と、前記コンテン

ツ送信手段は同一のＬＳＩに封止されていることを特徴とする請求項４に記載の中継装置。

【請求項７】前記第１のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第１の鍵情報と、前記第２のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第２の鍵情報とを同一のものとすることを特徴とする請求項４に記載の中継装置。

【請求項８】前記第１又は第２のいずれか他方のコンテンツ保護手段における前記コンテンツ保護の手続きは、所定の鍵情報を用いて、コンテンツ単位又はサービス単位又はサブユニット単位で行なうことを特徴とする請求項７に記載の中継装置。

【請求項９】前記第１及び第２のネットワーク上の装置又はサービス又はサブユニットから、該装置の認証フォーマットの有無を含む構成情報を受信する構成情報受信手段と、

前記構成情報受信手段で受信した各構成情報に基づいて、該装置又はサービス又はサブユニットの構成認識を行う構成認識手段とを更に具備したことを特徴とする請求項２または４に記載の中継装置。

【請求項１０】第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

前記第１のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第１のコンテンツ保護手段と、

前記第２のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第２のコンテンツ保護手段と、

前記第１又は第２のいずれか一方のネットワーク上の装置から、自中継装置上の装置又はサービス又はサブユニット宛であり、前記第１又は第２のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、

前記コンテンツ受信手段で受信したコンテンツを、前記第１又は第２のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第１又は第２のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備し、

前記第１のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第１の鍵情報と、前記第２のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第２の鍵情報とを同一のものとすることを特徴とする中継装置。

【請求項１１】ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、

前記ネットワーク上の他の装置に対して、自通信装置のアドレスを付与した暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは更に自通信装置のアドレスおよび該コンテンツを一意に識別可能な識別子を付与して、送信するコンテンツ送信手段と、

前記ネットワーク上の他の装置から、前記仮想チャネル上を介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはプラグについての問合せを受信する受信手段と、

この問合せに応答して、前記ネットワーク上の他の装置に対し、該当するサービスまたはサブユニットまたはプラグについての通知をする通知手段とを具備することを特徴とする通信装置。

【請求項１２】ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、

前記ネットワーク上の他の装置から、該ネットワーク上の他の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該ネットワーク上の他の装置が該コンテンツを一意に識別可能な識別子が付与された形で、受信するコンテンツ受信手段と、

前記ネットワーク上の他の装置に対して、前記仮想チャネルを介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはプラグについての問合せを送信する送信手段と、

前記ネットワーク上の他の装置から、前記問合せに該当するサービスまたはサブユニットまたはプラグについての通知を受信する受信手段とを具備することを特徴とする通信装置。

【請求項１３】ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置に対して、暗号化されたコンテンツを、送信アドレス、送信ポート、受信アドレスおよび受信ポートの組みで識別されるフローを介して送信または受信するコンテンツ転送手段と、

前記ネットワーク上の他の装置との間で、予め定められた論理ポートを用いて、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段とを具備し、

前記所定のコンテンツ保護手続きを行なう場合には、これを前記フローの単位で行なうことを特徴とする通信装置。

【請求項１４】前記所定のコンテンツ保護手続きに含ま

れる少なくとも一部の手続きにおいてやり取りされる情報に前記フローの識別子を付与することを特徴とする請求項２１に記載の通信装置。

【請求項１５】ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、

前記ネットワーク上の他の装置に対して、送信側の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該送信側の装置が該コンテンツを一意に識別可能な識別子を付与された形で、送信または受信するコンテンツ送受信手段とを具備し、

前記所定のコンテンツ保護手続きに含まれる少なくとも一部の手続きにおいてやり取りされる情報に、前記暗号化されたコンテンツのやり取りを行うサービス、サブユニット、仮想チャネルもしくはプラグの識別子、または前記送信側の装置が前記コンテンツを一意に識別可能な識別子のうちの少なくとも一つを付与することを特徴とする通信装置。

【請求項１６】第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

第１のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続き行う第１のコピープロテクション処理手段と、

第２のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続き第２のコピープロテクション処理手段と、

前記第１のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、

前記第１のインタフェース手段から受信された前記暗号化されたデータを、前記第１のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、

前記復号化されたデータを、別の符号化形式のデータに変換する変換手段と、

前記復号化されたデータを、前記第２のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、

前記暗号化されたデータを、前記第２のインタフェース手段へ転送するコンテンツ送信手段とを具備したことを特徴とする中継装置。

【請求項１７】前記第２のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第１のネットワーク側に開示するとともに、前記第１のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第２のネットワーク上の装置またはサービスまたはサブユニット宛に送信するとともに、

前記第１のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第２のネットワーク側に開示するとともに、前記第２のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第１のネットワーク上の装置またはサービスまたはサブユニット宛に送信する代理構成手段を更に具備し、

前記代理構成手段は、前記第１または第２の一方のネットワーク上の装置と、前記第１または第２の他方のネットワーク上の装置またはサービスまたはサブユニットとの、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行う場合には、前記第１または第２の一方のコピープロテクション処理手段を用いて前記一方のネットワーク上の装置と該所定のコンテンツ保護手続きを行うとともに、前記第１または第２の他方のコピープロテクション処理手段を用いて前記他方のネットワーク上の装置またはサービスまたはサブユニットと該所定のコンテンツ保護手続きを行うことを特徴とする請求項２４に記載の中継装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＩＥＥＥ１３９４バスや無線ネットワーク等のネットワーク間のデータ転送を中継する中継装置及びＩＥＥＥ１３９４バスや無線ネットワーク等のネットワークを介して通信を行う通信装置に関する。

【０００２】

【従来の技術】近年、デジタル放送の開始や、デジタルＡＶ機器の発売等、いわゆる「家庭ＡＶ環境のデジタル化」が大きな注目を集めている。デジタルＡＶデータは、様々な圧縮が可能、マルチメディアデータとしても処理が可能、何回再生しても劣化がない、等の優れた特徴を持ち、今後その用途はますます広がっていくものと考えられる。

【０００３】しかしながら、このデジタルＡＶ技術には、反面、「コンテンツの不正コピーが容易に行える」という側面もある。すなわち、どのようなデジタルコンテンツについても、原理的に「ビットのコピー」で、元どおりの品質の、しかも未来永劫にわたって一切劣化のない複製が作れてしまうため、いわゆる「不正コピー」の問題が発生する。

【０００４】この「不正コピー」を防ぐための技術がい

くつか検討されている。その中の一つが、CPTWG（コピープロテクション技術ワーキンググループ）で検討されている「1394CPコンテンツ保護システム仕様（1394CP Content Protection System Specification）」である。この技術は、IEEE1394バスに接続されたノード間で、転送するコンテンツ（例えばMPEGデータ等）について、送受信ノードの間で予め認証手続きを行い、暗号鍵（コンテンツキー）を共有できるようにしておき、以降は転送するコンテンツを暗号化して転送し、認証手続きを行った両者以外はコンテンツが読めないようにする技術である。このようにすることにより、認証手続きを行っていないノードは、コンテンツキーの値がわからないため、転送されているデータ（暗号化されているデータ）をたとえ取り込むことができたとしても、この暗号を復号化することはできない。このような認証に参加できるノードは、あらかじめ定められた認証機関が許可したノードのみとしておくことで、不正なノードが暗号鍵を入手することを未然に防ぎ、不正コピーを予め防ぐことが可能になる。

【0005】

【発明が解決しようとする課題】IEEE1394バスは、最低速度でも100Mbps、網そのものに自動構成認識機能が備わっている、QOS転送機能を持つ等、非常に優れた特徴を持つネットワークシステムであり、それゆえに家庭向けのデジタルAV向けのネットワークとして、デファクトスタンダードの地位を築いている。

【0006】しかし、IEEE1394は、これら特徴のゆえに、「IEEE1394と、他のネットワークを接続するとき」に様々な制約を生んでいる。例えば、無線網や公衆網とIEEE1394バスを接続する場合は、これらの網が100Mbps以上といった高速性を一般には有していないことや、IEEE1394の自動構成認識機能をこれらの網へそのまま拡張する、といった方法が簡単にはとれないことから、IEEE1394プロトコルをそのまま無線や公衆網に拡張する、といった方法を使うことはできない。そこで、IEEE1394と、無線網や公衆網などの他網の間にプロトコル変換ゲートウェイを配置し、相互接続する方法や、片方の網上のサービスをもう片方の網のサービスとして提供するいわゆる代理サーバの方法等が提案されている。

【0007】これらの方法を、従来の技術で述べた1394コピープロテクションに適用しようとした場合、現状では該コピープロテクション技術がIEEE1394バスについてのみ定められている状況である。このコピープロテクション技術を「IEEE1394と、他のネットワークを接続するとき」に拡張するための技術はないのが現状である。

【0008】本発明は、上記事情を考慮してなされたもので、コピープロテクション技術をIEEE1394のみならず、これと相互接続された他網にも拡張可能な中継装置及び通信装置を提供することを目的とする。

【0009】また、本発明は、同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とする中継装置及び通信装置を提供することを目的とする。

【0010】

【課題を解決するための手段】本発明（請求項1）に係る中継装置は、第1のネットワークに接続された第1のインタフェース手段と、第2のネットワークに接続された第2のインタフェース手段と、前記第2のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして前記第1のネットワーク側に開示する代理構成手段と、この装置又はサービス又はサブユニット宛の制御コマンド信号を前記第1のネットワーク側から受信する制御コマンド受信手段と、この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を前記第2のネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、前記第1のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記第2のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段とを具備したことを特徴とする。

【0011】本発明（請求項2）に係る中継装置は、第1のネットワークに接続された第1のインタフェース手段と、第2のネットワークに接続された第2のインタフェース手段と、第1及び第2のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして各々他方のネットワーク側に開示する代理構成手段と、この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、前記第1又は第2のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段と、前記第1又は第2のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛であり、前記コンテンツ保護情報から得られるコンテンツ鍵で保護

されたコンテンツを受信するコンテンツ受信手段と、このコンテンツ受信手段で受信した前記コンテンツに変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ転送手段とを具備したことを特徴とする。

【００１２】好ましくは、前記コンテンツ保護情報は、前記第１のネットワーク上の装置又はサービス又はサブユニットと、前記第２のネットワーク上の装置又はサービス又はサブユニット間の認証及び又は鍵交換を含むコンテンツ保護の手続きに関する情報であるようにしてもよい。

【００１３】本発明によれば、例えば、保護すべきコンテンツの送信もしくは受信を行っているペアである「代理構成手段が提供している第２のネットワーク上の装置またはサービスまたはサブユニット（以下、装置またはサービスまたはサブユニットを装置等と呼ぶ）」と「第１のネットワーク上の装置」との間において、「第１のネットワーク上の装置」または「代理構成手段が提供している第２のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「第１のネットワーク上の装置」または「代理構成手段が提供している第２のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、実際には、中継装置がその手続きを中身を変えることなく中継することによって、そのコンテンツ保護手続きを直接「代理構成手段が提供している第２のネットワーク上の装置等」と「第１のネットワーク上の装置」との間において行うことができる。

【００１４】また、本発明によれば、保護されるべきコンテンツを、その保護形式を変更することなく受信側に送り届けることができ、コンテンツを保護された形でエンドエンドに送り届けることができる。

【００１５】本発明（請求項４）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェース手段と、第１及び第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして各々他方のネットワーク側に開示する代理構成手段と、この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、前記第１のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第１のコンテンツ保護手段と、前記第２のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第２のコンテンツ保護手段と、前記第１又は第２のいずれか一方のネットワーク上の装置から、前記代理構成手段で開示した自中継装置上の装置又はサービス又はサブユニット宛であり、前記第１又は第２のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、前記コンテンツ受信手段で受信したコンテンツを、前記第１又は第２のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第１又は第２のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備したことを特徴とする。

【００１６】本発明によれば、例えば、保護すべきコンテンツの送信もしくは受信を行っているペアである「第２のネットワーク上の装置等」と「第１のネットワーク上の装置」との間において、「第１のネットワーク上の装置」または「第２のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「第１のネットワーク上の装置」または「第２のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、例えば、中継装置が、コンテンツ保護手続きをそれぞれ終端することで、結局、「第２のネットワーク上の装置等」と中継装置との間、および中継装置と「第１のネットワーク上の装置」との間で、コンテンツ保護手続きをそれぞれ行うこととなり、結局、エンドエンドでコンテンツの保護を行うことができる。

【００１７】また、第１のネットワーク上の装置から第２のネットワーク上の装置等の間の全ての経路において、転送されるデータは暗号化されていることになり、不正コピー等を未然に防ぐことが可能になる。

【００１８】好ましくは、前記第１のコンテンツ保護手段と、前記第２のコンテンツ保護手段で用いられる暗号化方式は異なる方式であるか、又は異なる鍵情報に基づくものであるようにしてもよい。

【００１９】好ましくは、前記コンテンツ受信手段と、前記コンテンツ送信手段は同一のＬＳＩに封止されているようにしてもよい。これによって、この復号化手段と暗号化手段との間は、暗号化されていないコンテンツデータが流れるため、個々にプローブをあてる等して、ここからコンテンツデータを盗聴し、不正コピーを働くことを未然に防止することが可能となる。

【００２０】好ましくは、前記第１のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第１の鍵情報と、前記第２のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第２の鍵情報とを同一のものとするようにしてもよい。これによって、一方のネットワークから伝えられた、他方のネットワーク

へ転送された暗号化データの鍵に関する情報（鍵やシード等）を、他方のネットワークへそのまま転送することにより、他方のネットワーク上の装置では該暗号化鍵の再生が可能となるため、コンテンツ受信手段とコンテンツ送信手段との間の暗号復号機能および再暗号化機能が不要となり、中継装置の大幅なコストの低減と、処理速度の高速化を図ることが可能となる。

【００２１】また、好ましくは、他方のネットワーク側の装置と、暗号化されたデータの転送を行っている場合には、他方のネットワーク上の他の装置からの、暗号化が必要なデータの送信要求は拒否するようにしてもよい。このようにすれば、他方のネットワーク側において、異なる暗号化されたデータ転送を未然に防止することが可能となる。

【００２２】好ましくは、前記第１又は第２のいずれか他方のコンテンツ保護手段における前記コンテンツ保護の手続きは、所定の鍵情報を用いて、コンテンツ単位又はサービス単位又はサブユニット単位で行なうようにしてもよい。これによって、他方のネットワーク側の装置との間で、複数の暗号鍵を定義できるようになるため、暗号化されたデータを同時に転送することが可能となり、一方のネットワーク上の装置から複数の暗号化データが転送される場合あるいは一方のネットワーク上に複数の装置がある場合等への対処が可能となる。

【００２３】好ましくは、前記第１及び第２のネットワーク上の装置又はサービス又はサブユニットから、該装置の認証フォーマット（機器証明）の有無を含む構成情報を受信する構成情報受信手段と、前記構成情報受信手段で受信した各構成情報に基づいて、該装置又はサービス又はサブユニットの構成認識を行う構成認識手段とを更に具備するようにしてもよい。これによって、代理構成手段が構成する代理サービスを、自動的に構成することができるようになり、もって、コンテンツ保護手続きに至る手順のプラグアンドプレイでの実現が可能になる。

【００２４】また、好ましくは、前記代理構成手段は、前記第１のネットワークの装置に対してデータを送信する際に、あらかじめ該第１のネットワークの装置に対して自中継装置が代理構成している該データを送信する装置またはサービスまたはサブユニットを通知するようにしてもよい。これによって、この通知を受信した第１のネットワーク上の装置に対して、どこに認証要求を出せばよいかを通知することが可能になる。

【００２５】本発明（請求項１０）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェース手段と、前記第１のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第１のコンテンツ保護手段と、前記第２のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第２のコンテンツ保護手段と、前記第１又は第２のいずれか一方のネットワーク上の装置から、自中継装置上の装置又はサービス又はサブユニット宛であり、前記第１又は第２のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、前記コンテンツ受信手段で受信したコンテンツを、前記第１又は第２のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第１又は第２のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備し、前記第１のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第１の鍵情報と、前記第２のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第２の鍵情報とを同一のものとすることを特徴とする。

【００２６】本発明（請求項１１）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、前記ネットワーク上の他の装置に対して、自通信装置のアドレスを付与した暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは更に自通信装置のアドレスおよび該コンテンツを一意に識別可能な識別子を付与して、送信するコンテンツ送信手段と、前記ネットワーク上の他の装置から、前記仮想チャネル上を介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはプラグについての問合せを受信する受信手段と、この問合せに応答して、前記ネットワーク上の他の装置に対し、該当するサービスまたはサブユニットまたはプラグについての通知をする通知手段とを具備することを特徴とする。

【００２７】本発明（請求項１２）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、前記ネットワーク上の他の装置から、該ネットワーク上の他の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該ネットワーク上の他の装置が該コンテンツを一意に識別可能な識別子が付与された形で、受信するコンテンツ受信手段と、前記ネットワーク上の他の装置に対して、前記仮想チャネルを介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはプラグについての問合せを送信する送信手段と、前記ネットワーク上の他の装置から、前記問合せに該当す

るサービスまたはサブユニットまたはプラグについての通知を受信する受信手段とを具備することを特徴とする。

【００２８】本発明によれば、特定の仮想チャネルで転送されている暗号化データの送信、あるいは受信それぞれのサブユニットあるいはプラグを特定することが可能となり、以降の認証・鍵交換で、「このサブユニット（あるいはプラグ）から送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。あるいは、本発明によれば、特定の識別子を持って転送されている暗号化データの送信、あるいは受信それぞれのサブユニットあるいはプラグを特定することが可能となり、以降の認証・鍵交換で、「このサブユニット（あるいはプラグ）から送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

【００２９】本発明（請求項１３）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置に対して、暗号化されたコンテンツを、送信アドレス、送信ポート、受信アドレスおよび受信ポートの組みで識別されるフローを介して送信または受信するコンテンツ転送手段と、前記ネットワーク上の他の装置との間で、予め定められた論理ポートを用いて、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段とを具備し、前記所定のコンテンツ保護手続きを行なう場合には、これを前記フローの単位で行なうことを特徴とする。

【００３０】好ましくは、前記所定のコンテンツ保護手続きに含まれる少なくとも一部の手続きにおいてやり取りされる情報に前記フローの識別子を付与するようにしてもよい。

【００３１】本発明によれば、フロー毎に異なる鍵の定義ができるようになるため、以降の認証・鍵交換で、「このフローに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

【００３２】本発明（請求項１５）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、前記ネットワーク上の他の装置に対して、送信側の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該送信側の装置が該コンテンツを一意に識別可能な識別子を付与された形で、送信または受信するコンテンツ送受信手段とを具備し、前記所定のコンテンツ保護手続きに含まれる少なくとも一部の手続きにおいてやり取りされる情報に、前記暗号化されたコンテンツのやり取りを行うサービス、サブユニット、仮想チャネルもしくはプラグの識別子、または前記送信側の装置が前記コンテンツを一意に識別可能な識別子のうちの少なくとも一つを付与することを特徴とする。

【００３３】本発明によれば、認証・鍵交換で、「このサブユニット、あるいはプラグ、あるいは仮想チャネルから送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。あるいは、本発明によれば、認証・鍵交換で、「このサブユニット、あるいはプラグから、あるいは前記特定の識別子を持って、送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

【００３４】本発明（請求項１６）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェース手段と、第１のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続き行う第１のコピープロテクション処理手段と、第２のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続き第２のコピープロテクション処理手段と、前記第１のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、前記第１のインタフェース手段から受信された前記暗号化されたデータを、前記第１のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、前記復号化されたデータを、別の符号化形式のデータに変換する変換手段と、前記復号化されたデータを、前記第２のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、前記暗号化されたデータを、前記第２のインタフェース手段へ転送するコンテンツ送信手段とを具備したことを特徴とする。

【００３５】本発明によれば、第１のネットワークを伝送させるデータが保護されるべきコンテンツであり、且つ、第１のネットワークと第２のネットワークの通信帯域が著しく異なる場合のように、第２のネットワークに元のデータとは異なるデータ形式で転送することが求め

られた場合に、変換手段によってデータ形式の変換を行いつつ、第1のネットワーク上の装置から第2のネットワーク上の装置等の間の全ての経路において、転送されるデータは暗号化されていることになり、両区間（両データ形式）においても、不正コピー等を未然に防ぐことが可能になる。

【0036】好ましくは、請求項16に記載の中継装置において、前記第2のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第1のネットワーク側に開示するとともに、前記第1のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第2のネットワーク上の装置またはサービスまたはサブユニット宛に送信するとともに、前記第1のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第2のネットワーク側に開示するとともに、前記第2のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第1のネットワーク上の装置またはサービスまたはサブユニット宛に送信する代理構成手段を更に具備し、前記代理構成手段は、前記第1または第2の一方のネットワーク上の装置と、前記第1または第2の他方のネットワーク上の装置またはサービスまたはサブユニットとの、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行う場合には、前記第1または第2の一方のコピープロテクション処理手段を用いて前記一方のネットワーク上の装置と該所定のコンテンツ保護手続きを行うとともに、前記第1または第2の他方のコピープロテクション処理手段を用いて前記他方のネットワーク上の装置またはサービスまたはサブユニットと該所定のコンテンツ保護手続きを行うようにしてもよい。

【0037】本発明によれば、保護すべきコンテンツの送信もしくは受信を行っているペアである「他方のネットワーク上の装置等」と「一方のネットワーク上の装置」との間において、「一方のネットワーク上の装置」または「他方のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「一方のネットワーク上の装置」または「他方のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、実際には、中継装置がそのコンテンツ保護手続きをそれぞれ終端することで、結局、「他方のネットワーク上の装置等」と中継装置、および中継装置と「一方のネットワーク上の装置」との間で、コンテンツ保護手続きを行うこととなり、結局、エンドエンドでコンテンツの保護を行うことができる。

【0038】また、好ましくは、請求項16に記載の中継装置において、前記コンテンツ受信手段は、前記第2のコピープロテクション処理手段を用いて、前記第2のネットワーク上の装置またはサービスまたはサブユニットと、前記所定のコンテンツ保護手続きのうち少なくとも一部を行ってそれが正常に終了した場合に、前記第1のコピープロテクション処理手段を用いて、前記第1のネットワークの装置またはサービスまたはサブユニットと前記所定のコンテンツ保護手続きのうち少なくとも一部を行うようにしてもよい。なお、前記所定のコンテンツ保護手続きのうち少なくとも一部は、例えば、認証手続きである。このようにすれば、第2のネットワーク上の装置またはサービスまたはサブユニットが信頼に足るデバイスであるかどうかを未然に知ることができるようになり、まず第2のネットワーク上の装置等と認証手続きを行い、その後、第1のネットワーク上の装置等との認証に失敗した場合に、第1のネットワーク上の装置等との認証を改めて行わなくてもよい分、通信資源や処理資源の節約になる。

【0039】また、本発明に係る通信装置は、第1の装置の制御に供される画面描画のためのプログラムを含む、第1の制御プログラムを受信し、これを稼働するプロセッサ手段と、このプロセッサ手段が描画する画面のうちの少なくとも一部を構成するパネル画面を作成する画面作成手段と、前記パネル画面へのコマンドと、前記第1の装置の制御のためのコマンドとの対応関係を記憶する記憶手段と、前記パネル画面をサブユニットとして第2の装置に公開するサブユニット処理手段と、前記サブユニットへのコマンドを受信した場合、前記記憶手段を参照してこのコマンドを前記第1の装置の制御のためのコマンドに変換して、これを送出する手段とを具備したことを特徴とする。一般に、前記のような制御プログラムを稼働させるためには、仮想マシンと呼ばれ計算環境を用意する必要があるのに対し、パネル画面を通した機器制御は、簡単なコマンド体型を用意するだけでよいため、簡単な計算環境を用意しておけばよい。本発明によれば、前記制御プログラムを持たない第2の装置に対しても、パネル画面という形で、前記第1の装置の制御インタフェースを提供することが可能になる。

【0040】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【0041】また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0042】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【００４３】（第１の実施形態）図１は、ある家庭のホームネットワークの全体構成の一例である。

【００４４】このホームネットワークには、送信ノード１０１、中継ノード１０２、無線ノード１０３の３つが接続されており、送信ノード１０１と中継ノード１０２は（有線の）ＩＥＥＥ１３９４バス１０４に、中継ノード１０２と無線ノード１０３は無線網にそれぞれ接続されている。ただし、後述するような方法で、各々のノードは互いに通信ができるようになっている。

【００４５】本実施形態では、送信ノード１０１から送出されたＭＰＥＧ映像を、中継ノード１０２で中継し、無線区間を経由して無線ノード１０３に送信する場合を例として説明する。その際に、著作権保護（不正コピーの防止）のために、送信ノード１０１と無線ノード１０３との間で転送されるＭＰＥＧ映像データは暗号化される場合を考える。

【００４６】なお、図１では、３つのノードを示してあるが、もちろん、これらの他にノードが接続されていてもよい（後述する他の実施形態においても同様である）。

【００４７】図２に、送信ノード１０１の内部構造の一例を示す。

【００４８】送信ノード１０１は、内部にＭＰＥＧ映像データを蓄積している装置であり、要求に応じてＭＰＥＧ映像データをＩＥＥＥ１３９４バス１０４を通じて送出する。その際、ＩＥＥＥ１３９４バス上において不法コピーをされることを未然に防止するために、必要な場合には送出するＭＰＥＧ映像データを暗号化して送出する機能を持つ。そのため、ＭＰＥＧ映像データを受信するノードと、認証データ、暗号鍵等の交換を行うための機構も持つ。

【００４９】図２に示されるように、この送信ノード１０１は、ＩＥＥＥ１３９４インタフェース４０１、ＡＶ／Ｃプロトコルの処理を行うＡＶ／Ｃプロトコル処理部４０２、ＡＶ／Ｃプロトコル内のコピープロテクションに関する処理を行うコピープロテクション処理部４０３、ＩＥＥＥ１３９４を通して送受信されるデータのうち、同期チャネルを通してやり取りされるデータについて送受信するＩＳＯ信号送受信部４０４、ＭＰＥＧ映像のストレージであるＭＰＥＧストレージ部４０６、コピープロテクション処理部４０３から暗号鍵Ｋをもらい、ＭＰＥＧ映像を暗号化してＩＳＯ信号送受信部４０４に送出する暗号化部４０５を有する。ここで、コピープロテクション処理部４０３は、認証のためのフォーマットＡｃｅｒｔを持つ。

【００５０】次に、図３に、中継ノード１０２の内部構造の一例を示す。

【００５１】中継ノード１０２は、ＩＥＥＥ１３９４バス側から受信したデータ（ＭＰＥＧ映像データ）を無線区間側にフォワードする機能の他に、ＩＥＥＥ１３９４バス側のノードに対して無線ノードの代理サーバとなり、無線ノードの機能を代理で提供する機能、および無線区間側のノードに対してＩＥＥＥ１３９４バス側のノード（本実施形態では送信ノード１０１）の代理サーバとなり、ＩＥＥＥ１３９４バス側のノードの機能を代理で提供する機能が存在する。

【００５２】図３に示されるように、この中継ノード１０２は、ＩＥＥＥ１３９４インタフェース２０１、無線インタフェース２０２、ＡＶ／Ｃプロトコル処理部２０３、ＩＳＯ信号送受信部２０４、無線区間側の同期チャネルの信号の送受信を行う無線ＩＳＯ信号送受信部２０５、ＩＥＥＥ１３９４バス上のノードの構成情報を収集したり、自らの構成情報（自分がどのような機能を持っているかについての情報等）をＩＥＥＥ１３９４上に広告する機能を持つ１３９４バス構成認識部２０６、ＩＥＥＥ１３９４バス側に対して無線区間側のノードやサービス（サブユニット）を代理で公開したり、無線区間側のノードやサービスへのコマンド等を代理で受け付け、これを無線区間側に必要に応じてプロトコル変換をして送出したり、あるいは無線区間側に対してＩＥＥＥ１３９４側のノード／サービス（サブユニット）の代理公開やコマンドの代理受付／翻訳等を行う代理サブユニット構成部２０７、無線区間上のノードの構成情報を収集したり、自らの構成情報（自分がどのような機能を持っているかについての情報等）を無線区間上に広告する機能を持つ無線区間構成認識部２０９、コピープロテクションに関する処理を行い、１３９４バスと無線区間をまたがるコピープロテクション処理に関しては、やり取りされる情報を透過的にフォワードさせるコピープロテクション制御／フォワード部２１０、無線区間でやり取りされる制御パケットの送受信を行う無線ノード制御パケット送受信部２１１を有する。

【００５３】次に、図４に、無線ノード１０３の内部構造の一例を示す。

【００５４】無線区間においていわゆるＩＥＥＥ１３９４プロトコル（物理レイヤプロトコル、リンクレイヤプロトコル等）が稼働している必要は必ずしもなく、ＩＥＥＥ８０２．１１や無線ＬＡＮ等、任意の無線プロトコルを利用することを想定するが、本実施形態では、特に、いわゆるＱＯＳ機能（同期通信機能）を持つ無線網であることを仮定する。ただし、本実施形態は、無線区間部分にＱＯＳ機能が求められると制限されるものではない。

【００５５】いわゆるＩＥＥＥ１３９４ノードではない無線ノード１０３が、ＩＥＥＥ１３９４バスにつながれたノード（本実施形態では送信ノード１０１）と通信を行うために、前述のように、中継ノード１０２がＩＥＥＥ１３９４バス上のノードや機能（サブユニット）をエ

ミュレートしている。すなわち、無線ノード１０３から見て、中継ノード１０２はいわゆるＩＥＥＥ１３９４バス側のノードや機能の代理サーバとなっている。無線ノード１０３は、これら（ＩＥＥＥ１３９４側のノードや機能）を中継ノード１０２の機能と考え、通信を行うが、実際には中継ノード１０２が必要なプロトコル変換やデータの乗せ換えを行う。

【００５６】図４に示されるように、この無線ノード１０３は、無線インタフェース３０１、無線ノード制御パケット送受信部３０２、コピープロテクション処理部３０３、無線ＩＳＯ信号送受信部３０４、受信した暗号化されたストリーム（ＭＰＥＧ映像等）を、コピープロテクション処理部３０３から渡されるコンテンツキーＫを使ってこれを復号化する暗号復号化部３０５、ＭＰＥＧデコード部３０６、映像を表示するディスプレイ部３０７を有する。

【００５７】無線ノード１０３のコピープロテクション処理部３０３は、後述するように、認証フォーマットＢｃｅｒｔを持ち、その認証の発行機関は、送信ノード１０１（の映像送出サブユニット）の認証フォーマットＡｃｅｒｔの発行機関と同一の発行機関である。

【００５８】次に、実際のコピープロテクションを施した上でのＭＰＥＧ映像全体のシーケンスについて、図５／図６（全体のシーケンス例）、図７／図８（送信ノード１０１のフローチャート例）、図９／図１０／図１１（中継ノード１０２のフローチャート例）、図１２／図１３（無線ノード１０３のフローチャート例）を参照しながら説明する。

【００５９】まず、無線ノード１０３は、自分の構成情報を中継ノード１０２に通知する（ステップＳ５０１）。この通知は、無線ノード内にＩＥＥＥ１２１２レジスタを用意し、ここに自分の構成情報を記しておく形で行われてもよい。構成情報とは、自分（無線ノード）がＭＰＥＧデコード／ディスプレイ機能を持つといったことや、認証・鍵交換のための認証フォーマットを持っていること、などである。ここで、この認証フォーマットが、特定のコピープロテクション機関が定めたフォーマットであることを同時に通知したり、ＩＥＥＥ１３９４向けのコピープロテクションのための認証フォーマットである旨を同時に通知してもよい。

【００６０】ここで、認証について簡単に説明する。

【００６１】ネットワーク上を映画やテレビ番組などの著作権を考慮すべきコンテンツ（データ）を転送する場合、それらのコンテンツは暗号によって保護を行うべきである。なぜなら、これらのデータの転送中に、ネットワーク上で盗聴された場合、不正コピーが可能となってしまうからである。これに対する対策としては、転送するデータの暗号化が有効である。

【００６２】次に問題となるのが、「怪しいものにデータを送っている危険はないか」という問題である。たとえ、データを暗号化して送ったとしても、送った先のノード（暗号を解く鍵を持っている）が悪意を持っている場合（不正コピーをしようと考えている場合）には、やはり解読可能な形でデータを送るべきではない。これに対する対策が認証である。すなわち、この暗号を解く鍵を受信側に渡す前に、受信側が不正を働かないものかどうかの確認をとる（確認が取れた受信側ノードにのみ暗号を解く鍵を渡す）仕組みである。

【００６３】具体的には、予め認証機関が「このノード（あるいはサブユニット）は、不正に働くことはない」と認定したノード（あるいはサブユニット）に対して、「認証フォーマット」と呼ばれるデータを、あらかじめ送信側のノードと受信側のノードとの両方に与えておく。この「認証フォーマット」を正しい形で持っているということは、そのノード（あるいはサブユニット）は信用できる（不正を働かない）と考えることができる。そこで、上記のデータ転送に先立って、送受信ノード（あるいはサブユニット）間で認証フォーマットのやり取りを行い、正しい形で認証フォーマットが確認できた場合に限り、暗号を解くための鍵（もしくは鍵を生成するための元となるデータ）を通知し、その鍵で暗号化されたデータをネットワーク上を転送する、という手法をとる。

【００６４】さて、無線ノード１０３は、このような認証フォーマットをあらかじめ認証機関により与えられており、「暗号化データを正当な形で受信／再生する権利」を持っている。ここで、無線ノード１０３が持っている認証フォーマットを「Ｂｃｅｒｔ」とする。

【００６５】無線ノード１０３は、図５のステップＳ５０１で自分の構成情報を通知する際に、自分は認証フォーマットを有していることを、この構成情報に加えてもよい（ステップＳ８０１）。例えば、図１４のように、構成情報の中に、本無線ノード１０３がＭＰＥＧデコード／ディスプレイ機能を持っており、さらに該機能が認証フォーマットを持っていること、その認証フォーマットがどの発行機関が発行したものか、等の情報を有する。

【００６６】なお、中継ノード１０２が無線ノード１０３の構成を認識する方法としては、この他にも中継ノード１０２が無線ノード１０３に対して構成を問い合わせるパケットを送信し、無線ノード１０３がこれに答える方法等も可能である。

【００６７】さて、この構成情報を受信した中継ノード１０２は、無線ノード１０３が認証フォーマットを持つことや、ＭＰＥＧデコード／ディスプレイ機能を持っていることを確認する（ステップＳ７０１）。

【００６８】中継ノード１０２は、無線ノード１０３がＭＰＥＧデコード／ディスプレイ機能を持っていることをＩＥＥＥ１３９４バス側のノードに対して知らせるため、このＭＰＥＧデコード／ディスプレイ機能を、中継

ノード102自身のサブユニットとしてIEEE1394バス側に広告する（ステップS502）。具体的には、IEEE1212レジスタに「自分はMPEGデコード／ディスプレイ機能を持っている」旨を記載したり、AV／Cプロトコルでサブユニット構成の問い合わせを受けた場合に、自分がMPEGデコード／ディスプレイサブユニットを持っているという形で応答を返したりする（これにより、IEEE1394に接続されたノードは、中継ノード102にこの機能が存在すると認識することになる）。

【0069】そのために、中継ノード102は、代理サブユニット構成部207内に代理テーブル208を持つ。代理テーブル208は、図15／図16のように、中継ノード102が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【0070】ここでは、図15のように、無線ノード103のMPEGデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップS702，S703）。

【0071】このため、送信ノード101から見た中継ノード102の構造は図17のように見えることになる（ステップS601）。

【0072】以上は、IEEE1394バス側についての説明であったが、これと同様の関係が無線区間にも成り立っている。すなわち、中継ノード102は、IEEE1394バス側の機器やサービス、サブユニット構成等を調査し、これらの代理サービスを無線区間側に行っている。よって、図16のような設定がなされ、無線ノードから見た中継ノード102の構造は図18のように見える。

【0073】さて、中継ノード102内にMPEGデコード／ディスプレイサブユニットがあると認識した送信ノード101は、このサブユニットに対して、MPEG映像を転送することを目的に、1394バス上に同期チャネル#xを確立し、AV／Cプロトコルにて「この同期チャネル#x（を受信するプラグ（例えば1394TAにて規定されたAV／Cにおけるプラグ））と、MPEGデコード／ディスプレイサブユニットとを接続し、映像を表示せよ」との命令をだす（ステップS503，S602）。送信ノード101は、このサブユニットが中継ノード101にあたるものと解釈しているため、命令の送信先は中継ノード102である。

【0074】これを受信（ステップS704）した中継ノード102は、受信した命令パケットを解釈し、その命令が自らが代理サービスを行っているMPEGデコード／ディスプレイサブユニットに対する命令であることを認識し、代理テーブル208を参照して、この命令先の実体は無線ノード103にあることを認識する（ステップS705）。

【0075】よって、IEEE1394バスの同期チャネル#xを通して受信したデータを、無線ノード側にフォワードすべく、無線区間の同期チャネル（#y）の確保を行い（ステップS706）、さらにISO信号送受信部204（同期チャネル#xを受信）と無線ISO信号送受信部205（同期チャネル#yを送信）を接続し、1394インタフェース201から入力された入力データ（ISOデータ）を無線区間にフォワードできるようにする（ステップS504，S707）。

【0076】さらに、無線ノード103に対して、「無線同期チャネル#yを通してデータを送信するので、これを受信し、MPEGデコーダに入力し、その結果をディスプレイに表示せよ」との命令を、無線ノード制御パケットの形で送信する（ステップS505，S708）。

【0077】図19に、この無線ノード制御パケットの一例を示す。

【0078】図19に示されるように、無線ノード103に無線同期チャネル#yを通して送信したデータ（MPEG映像）を、MPEGデコード／ディスプレイ機能に転送し、表示することを促す内容となっている。また、この中にこのデータ（MPEG映像）を送信するサブユニット（中継ノード102の映像送信機能；実際には、送信ノード101の代理でその機能を持っていると広告している）についての情報も併せて通知している。

【0079】これを受信した無線ノード103は、無線同期チャネル#yを通してデータが送られてくることを認識する（ステップS802）。無線ノード103は、このデータの送信元は中継ノード102の映像送信サブユニットであると認識する（前述のように、実際のデータ送信元は送信ノード101である）。このため、この無線ノード制御パケット内に、「この無線同期チャネルを通して送信されるデータの送信元は中継ノード102の映像送信サブユニットである」との情報を含めてもよい。

【0080】この後、送信ノード101は、同期チャネル#xを通して、暗号化されたMPEG映像を転送する（ステップS603，S506）。これを受信した中継ノード102は、先に設定したようにこれを無線区間にフォワードする（ステップS709，S507）。

【0081】中継ノード102は、ステップS506で暗号化されたMPEG映像を受信した時点で、これが暗号化データであることを認識できるが、無線網側に転送する必要があると認識し、これをそのままフォワードする。後に認証・鍵交換の手続きが必要である旨を記憶しておいてもよい。

【0082】このようにして、暗号化されたMPEG映像が無線ノード103に到達する（ステップS803）。このMPEG映像には、ソースアドレスとして中継ノード102のノードIDが含まれていてもよい。このため、無線ノード103は、このMPEG映像が中継

ノード１０２から到達したものであることまでは認識できるが、この時点で無線ノード１０３はこの暗号を解くための鍵Ｋを有していない（もしくはその鍵を生成するための元となるデータを有していない）ため、この状態で暗号を解いて、ＭＰＥＧ映像を取り出すことはできない。ここで、無線ノード１０３は認証手続きがＭＰＥＧ映像の送信元と必要であることを認識する。

【００８３】そこで、無線ノード１０３（のコピープロテクション処理部３０３）は、認証要求を暗号化データの送信元に対して送信する。先に述べたように、無線ノード１０３には、上記暗号化データの送信元は中継ノード１０２（内の、サブユニット種別＝映像送信サブユニット、かつ、サブユニットＩＤ＝ｂ（ｂ＝０とする）の、サブユニット）であるように認識されている。

【００８４】また、図5のＳ５２１のように、中継ノード１０２に対して、「無線ノードにおいて、無線同期チャネル＃ｙを受信しているのは、サブユニット種別＝ＭＰＥＧデコード／ディスプレイサブユニットで、かつ、サブユニットＩＤ＝ｃ（ｃ＝０とする）の、サブユニットである。無線同期チャネル＃ｙに暗号化データを送信しているのはどのサブユニットか？」という意味合いの問い合わせを送信してもよい。これに対し、中継ノード１０２は、「無線同期チャネル＃ｙに送信しているのは、映像送信サブユニットのサブユニットＩＤ＝０である。」との返答を返す（ステップＳ５２２，Ｓ７３１，Ｓ８３１）。これにより、無線ノード１０３は、認証を行なう先が中継ノードの映像送信サブユニットであることを認識できる。

【００８５】このように、認証要求の宛先を認識し、中継ノード１０２（内の映像送信サブユニットのサブユニットＩＤ＝０）に対し、認証要求を送信する。この送信の仕方として、認証要求パケットの宛先を「中継ノードの映像送信サブユニット（のサブユニットＩＤ＝０）」としてもよいし、認証要求パケットの任意の位置に「映像送信サブユニット（のサブユニットＩＤ＝０）」という情報を入れ、認証要求先は映像送信サブユニット（のサブユニットＩＤ＝０）であると言うことを明確に表示してもよい。前者の場合は、中継ノードの各サブユニット内に認証・鍵交換の手続きが含まれていることを意味する。後者の場合は、中継ノードのある特定の処理部が、一括して、各サブユニットの認証・鍵交換を行なうことを意味する。

【００８６】その際、認証要求には、無線ノード１０３の認証フォーマットＢｃｅｒｔを付与する（ステップＳ８０４，Ｓ５０８）。Ｂｃｅｒｔは、無線ノード１０３のＭＰＥＧデコード／ディスプレイサブユニットの認証フォーマットであってもよい。なお、コピープロテクション処理部は、サブユニット毎（サブユニット種別毎）でなく、サブユニットＩＤ毎に認証フォーマットを用意してもよい。

【００８７】認証要求を受信（ステップＳ７１０）した中継ノードは、代理テーブル２０８を参照して、この認証要求の要求先が実は送信ノード１０１（の映像送信サブユニットのサブユニットＩＤ＝ａ（ａ＝０とする））であることを認識する。

【００８８】中継ノード１０２は、送信ノード１０１に対して、「中継ノードにおいて、同期チャネル＃ｘを受信しているのはＭＰＥＧデコード／ディスプレイサブユニットのサブユニットＩＤ＝０である。同期チャネル＃ｘに暗号化データを送信しているのは、送信ノードのどのサブユニットか？」という意味合いの問い合わせを送信してもよい（ステップＳ５２３，Ｓ６３１，Ｓ７３２）。これに対し、送信ノード１０１は、「同期チャネル＃ｘに送信しているのは、映像送信サブユニットのサブユニットＩＤ＝０である。」との返答を返す（ステップＳ５２４，Ｓ６３１，Ｓ７３２）。

【００８９】このようにして、認証要求の相手を認識したならば、ステップＳ５０８にて受信した認証要求を、中身を変えずに（Ｂｃｅｒｔ等はそのまま残して）送信ノード１０１に対してフォワードする（ステップＳ５０９，Ｓ７１１）。すなわち、宛先アドレスや、認証要求の宛先であるサブユニット以外の認証フォーマット等は、中継ノードは透過的に転送できる。

【００９０】認証要求の転送の際は、先に説明したように、認証要求パケットの宛先を映像送信サブユニット（のサブユニットＩＤ＝０）としてもよいし、認証要求パケットの任意の位置に当該サブユニットを明示する情報を入れ、認証要求先は当該サブユニットであると言うことを明確に表示してもよい。

【００９１】ここで、認証要求の中身を変えずにフォワードすることで、この認証要求はそのままの形で送信ノード１０１に到達することになり、結局、送信ノード１０１と無線ノード１０３との間で、実際の認証手続きは進んでいくことになり、しかも中継ノード１０２をはじめ、その他のノードにはその認証の結果明らかになる鍵の値などの情報を知られることなく、以上の手続きを行っていくことが可能である。

【００９２】認証要求を受け取った送信ノード１０１は、これを中継ノード１０２のＭＰＥＧデコード／ディスプレイサブユニットから送られてきた認証要求であると解釈する（ステップＳ６０４）。その後、Ｂｃｅｒｔから無線ノード１０３のＭＰＥＧデコード／ディスプレイサブユニットを特定できるＩＤ（Ｂｄｉｄ）を抽出し（ステップＳ６０５）、これとともに、やはり同様の認証要求を認証要求の送信元に対して行おうとする。ただし、送信ノード１０１は、Ｂｃｅｒｔが無線ノード１０３の認証フォーマットであるとは意識することはなく、むしろ中継ノード１０２（のＭＰＥＧデコード／ディスプレイサブユニット）の認証フォーマットであると意識をしている。

【００９３】この認証要求には、送信ノード１０１（の映像送出サブユニット）の認証フォーマットＡｃｅｒｔと、Ｂｄｉｄとが含まれる。ここで、送信ノード１０１は、該認証要求（ステップＳ５０９）の送信元は中継ノード１０２（のＭＰＥＧデコード／ディスプレイサブユニット）であると解釈しているため、この認証要求の送信先はやはり中継ノード１０２となる（ステップＳ６０６，Ｓ５１０）。

【００９４】これを受信（ステップＳ７１２）した中継ノード１０２は、代理テーブル２０８を参照して、この認証手続の本来の要求先が無線ノード１０３（のＭＰＥＧデコード／ディスプレイ機能）であることを認識し、この認証手続要求を、中身を変えずに（Ａｃｅｒｔ等はそのまま残して）無線ノード１０３に対してフォワードする（ステップＳ５１１，Ｓ７１３）。この認証要求の送信元は中継ノード１０２である。

【００９５】これを受け取った無線ノード１０３は、これを中継ノード１０２の映像送信サブユニットから送られてきた認証要求であると解釈する（ステップＳ８０５）。その後、Ａｃｅｒｔから送信ノード１０１の映像サブユニットを特定できるＩＤ（Ａｄｉｄ）を抽出し、認証鍵の交換に必要な残りの手続きを、認証要求の送信元に対して行おうとする。なお、この場合も、無線ノード１０３は、Ａｃｅｒｔが送信ノード１０１の認証フォーマットであるとは意識せず、むしろ中継ノード１０２（の映像送信サブユニット）の認証フォーマットであると意識する。

【００９６】この認証鍵の交換に必要な残りの手続きとして、無線ノード１０３は、認証要求の送信元（と無線ノードが解釈しているノード）に対して認証・鍵交換手続きパケットを送信する（ステップＳ５１２）。この認証・鍵交換手続きパケットには、鍵交換初期値、署名、Ａｃｅｒｔの中に含まれていた送信ノード（の映像送信サブユニット）のデバイスＩＤ（Ａｄｉｄ）等が含まれている（ステップＳ８０６）。ここで、無線ノード１０３は、該認証要求（ステップＳ５１１）の送信元は中継ノード１０２（の映像送信サブユニット）であると解釈しているため、この認証要求の送信先はやはり中継ノード１０２となる。

【００９７】これを受信した中継ノード１０２は、代理テーブル２０８を参照して、この認証手続きの本来の要求先が送信ノード１０１（の映像送信サブユニット）であることを認識し、この認証手続きパケットを、中身を変えずに送信ノード１０１に対してフォワードする（ステップＳ５１３，Ｓ７１４）。このパケットの送信元は中継ノード１０２である。

【００９８】これと同様の手続きが送信ノード１０１→中継ノード１０２→無線ノード１０３の方向に対しても行われる（ステップＳ５１４，Ｓ５１５，Ｓ６０９，Ｓ７１５，Ｓ８０７）。

【００９９】この認証手続きパケットを受信した送信ノード１０１および無線ノード１０３は、それぞれ、受信したパケットが改ざんされていないかどうかのタンパの確認、相手から送られてきた認証フォーマットが正しいものであるかどうかの確認等を行い、与えられた値を使って共通の認証鍵Ｋａｕｔｈを導き出す。この共通の認証鍵Ｋａｕｔｈは、送信ノード（の映像送信サブユニット）と無線ノード（のＭＰＥＧデコード／ディスプレイ機能）との間で共通に持つ鍵で、この鍵Ｋａｕｔｈを、この両者（送信ノード１０１、無線ノード１０３）以外の他人に知られることなく共有することがこの時点でできるようになる（ステップＳ６０７，ステップＳ６０８，Ｓ８０８）。

【０１００】この認証鍵Ｋａｕｔｈを使って、実際にＭＰＥＧストリームの暗号化を行うコンテンツキーＫの計算ができるようになる。具体的な手順はここでは省略するが、送信ノード１０１から無線ノード１０２に、ＩＥＥＥ１３９４のコピープロテクション方式（５Ｃ方式）のように、交換鍵やシード（種）の値を別途送ることにより、コンテンツキーＫの計算ができるようになっていてもよい（ステップＳ５１８，Ｓ５１９）。

【０１０１】さて、このようにして、送信ノード１０１（の映像送信サブユニット）と無線ノード１０３（のＭＰＥＧデコード／ディスプレイ機能）との間で、コンテンツキーＫの値が共有できるようになった。

【０１０２】ここで、送信ノード１０１が、送信するＭＰＥＧ映像を、コンテンツキーＫを使って、暗号化部４０５にて暗号化し（ステップＳ６１０）、これを１３９４バスの同期チャネル＃ｘを通して中継ノード１０２（のＭＰＥＧデコード／ディスプレイサブユニット）に対して送信する（ステップＳ５１６，Ｓ６１１）。

【０１０３】中継ノード１０２は、送信ノード１０１から同期チャネル＃ｘを通して送られてくる暗号化されたＭＰＥＧ映像を、ＩＳＯ信号送受信部２０４から無線ＩＳＯ信号送受信部２０５を通して、無線同期チャネル＃ｙに送信する（ステップＳ５１７，Ｓ７１６）。

【０１０４】これを受信した無線ノード１０３は、キーＫの値を使ってＭＰＥＧ映像の値を復号化する（ステップＳ８０９，ステップＳ８１０）。復号化されたＭＰＥＧデータは、ＭＰＥＧデコード部３０６にて復号化され（ステップＳ８１１）、これをディスプレイ部３０７にて再生表示する（ステップＳ８１２）。

【０１０５】このように、１３９４バスと無線網との間に代理ノードが存在するような相互接続の環境においても、エンドーエンドのノード同士（本実施形態では送信ノード１０１と無線ノード１０３）が認証手続きや鍵交換手続きを行うことができ、さらにその内容を中継ノード１０２を含め、その他のノードが知ることはできない仕組みとなっている。また、実際のＭＰＥＧ映像等のコンテンツ保護の必要なデータの転送も、コピーが不可能

なように経路の全てで暗号化されており、安全なデータ転送が可能になっている。これによって、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【０１０６】なお、以上の実施形態は、認証手続きや、暗号鍵の交換手続き等を、ノードのサブユニット単位で行ってきたが、無線ノード単位でこれを行うことも可能である。なお、ノード単位で行う例については、次の第２の実施形態で説明するので、例えばこれを適用すればよい。

【０１０７】また、以上の実施形態では、認証および鍵交換のための手続きを暗号化データの受信後に行ってきたが、該手続きは、暗号化データ受信に先だって行ってももちろん構わない。例えば、装置や該当アプリケーションの立ち上げ時に該手続きを行ってもよい。

【０１０８】（第２の実施形態）次に、第２の実施形態について説明する。

【０１０９】第１の実施形態では、送信ノードと無線ノードとが、直接、互いに認証手続きや鍵交換手続きを行ってきた。すなわち、送信ノード（の映像サブユニット）と無線ノード（のＭＰＥＧデコード／ディスプレイ機能）とが、直接、互いを認証し、暗号鍵の交換手続きを行って、暗号化データのやり取りを行ってきた。この際、中継ノードは、送信ノードに対しては無線ノードのＭＰＥＧデコード／ディスプレイ機能の代理機能を果たし、無線ノードに対しては送信ノードの映像送信サブユニットの代理機能を果たしてきたが、上記の認証手続きおよび暗号化データのやり取りの部分については、これらのデータの単なるフォワードを、代理していたサブユニットなり機能なりに行う形であった。

【０１１０】これに対し、第２の実施形態では、中継ノードにて、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りを終端する場合の例を示す。すなわち、送信ノードと中継ノードとの間、および中継ノードと無線ノードとの間で、各々のコピープロテクション手続きは閉じている。つまり、この実施形態においても、中継ノードは、送信ノードあるいは無線ノードに対して代理サービスは提供するものの、コピープロテクションについては、中継ノード自身が認証フォーマットを持ち、中継ノード自身が、１３９４バス区間のＭＰＥＧデータの暗号化転送についての責任を終端するとともに、無線区間のＭＰＥＧデータの暗号化転送についての責任を終端する場合の例である。

【０１１１】図２０に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第１の実施形態と同様である。

【０１１２】図２１に、送信ノード２１０１の内部構造の一例を示す。これも第１の実施形態と基本的には同様である。

【０１１３】次に、図２２に、中継ノード２１０２の内部構造の一例を示す。

【０１１４】中継ノード２１０２は、第１の実施形態と同様に、ＩＥＥＥ１３９４バス側のノードに対して無線ノードの代理サーバとなり、無線ノードの機能を代理で提供する機能、および無線区間側のノードに対してＩＥＥＥ１３９４バス側のノード（本実施形態では送信ノード２１０１）の代理サーバとなり、ＩＥＥＥ１３９４バス側のノードの機能を代理で提供する機能を持つ。

【０１１５】また、ＩＥＥＥ１３９４バス側から受信したデータ（ＭＰＥＧ映像データ）を無線区間側にフォワードする機能を持つが、第１の実施形態と相違する点は、認証データや暗号化等、コピープロテクションに関する手続きがＩＥＥＥ１３９４バス区間と無線区間との両方について、この中継ノード２１０２において終端されており、ＩＥＥＥ１３９４バス側については認証フォーマットＢｃｅｒｔをＩＥＥＥ１３９４コピープロテクション処理部２２０８に、無線区間側については認証フォーマットＣｃｅｒｔを無線区間コピープロテクション処理部２２１２にそれぞれ持ち、１３９４バスの同期チャネルから入力されてきた暗号化データについては、ＩＳＯ信号受信部２２０３にて受信→暗号復号化部２２０４にて暗号復号化→復号化されたＭＰＥＧ映像を、暗号化部２２０５にて再暗号化→無線ＩＳＯ信号送受信部２２０６にて、無線同期信号上に送信、というプロセスを踏む点である。

【０１１６】これらの認証フォーマットは、ＩＥＥＥ１３９４インタフェース毎、あるいは無線区間インタフェース毎に１つずつもっていてもよいし、（代理も含めて）サブユニット毎（サブユニット種別毎）に１つずつ持っていてもよい。

【０１１７】ここで、ＡｃｅｒｔとＢｃｅｒｔは、同じ認証機関（例えばＩＥＥＥ１３９４のコピープロテクションを担当する認証機関）が発行した認証フォーマットであると仮定するが、後述する無線区間の認証フォーマット（後述するＣｃｅｒｔとＤｃｅｒｔ）については、同じくこの認証機関が発行したものであってもよいし、無線区間を担当する別の認証機関が発行する認証フォーマットであってもよい。

【０１１８】次に、図２３に、無線ノード２１０３の内部構造の一例を示す。コピープロテクション処理部２３０３が、無線区間向けの認証フォーマットＤｃｅｒｔを持っていること以外は、基本的には第１の実施形態の無線ノードと同様である。

【０１１９】次に、実際のコピープロテクションを施した上でのＭＰＥＧ映像全体のシーケンスについて、図２４／図２５（全体のシーケンス例）、図２６／図２７（送信ノード２１０１のフローチャート例）、図２８／図２９／図３０／図３１（中継ノード２１０２のフローチャート例）、図３２／図３３（無線ノード２１０３のフローチャート例）を参照しながら説明する。

【0120】まず、無線ノード2103は、自分の構成情報を中継ノード2102に通知する（ステップS2501）。構成情報とは、自分（無線ノード）がMPEGデコード／ディスプレイ機能を持つこといったことや、認証のための認証フォーマットを持っていることなどである（図14参照）。ここで、認証のための認証フォーマットが、無線区間用の認証フォーマットである旨を通知してもよい（ステップS2801）。

【0121】これを受信した中継ノード2102は、無線ノード2101が認証フォーマットを持つことや、MPEGデコード／ディスプレイ機能を持っていることを確認する（ステップS2701）。中継ノード2102は、第1の実施形態と同様に、このMPEGデコード／ディスプレイ機能を、IEEE1212レジスタやAV／Cプロトコル等を使って、中継ノード2102自身のサブユニットとしてIEEE1394バス側に広告する（ステップS2502）。

【0122】そのために、中継ノード2102は、代理サブユニット構成部2210内に代理テーブル2214を持つ。この代理テーブル2214は、基本的には第1の実施形態と同様であり、図34／図35のように、中継ノード2102が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【0123】ここでは、図34のように、無線ノード2103のMPEGデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップS2702，S2703）。

【0124】このため、送信ノード2101から見た中継ノード2102の構造は、図36のように見えることになる（ステップS2601）。

【0125】以上は、IEEE1394バス側についての説明であったが、第1の実施形態と同様に、これと同様の関係が無線区間にも成り立っている。すなわち、中継ノード2102は、IEEE1394バス側の機器やサービス、サブユニット構成等を調査し、これらの代理サービスを無線区間側に行っている。よって、図35のような設定がなされ、無線ノードから見た中継ノード2102の構造は図37のように見える。

【0126】さて、中継ノード2102内にMPEGデコード／ディスプレイサブユニットがあると認識した送信ノード2101は、このサブユニットに対して、MPEG映像を転送することを目的に、1394バス上に同期チャンネル#xを確立し、AV／Cプロトコルにて「この同期チャネル#x（を受信するプラグ）と、MPEGデコード／ディスプレイサブユニットとを接続し、映像を表示せよ」との命令を出す（ステップS2503，S2602）。送信ノード2101は、このサブユニットが中継ノード2102にあるものと解釈しているため、命令の送信先は中継ノード2102である。

【0127】これを受信（ステップS2704）した中継ノード2102は、受信した命令パケットを解釈し、その命令が自らが代理サービスを行っているMPEGデコード／ディスプレイサブユニットに対する命令であることを認識し、代理テーブル2210を参照して、この命令先の実体は無線ノード2103にあることを認識する（ステップS2705）。

【0128】ここで、図20の無線区間は、QOS対応の無線LANになっており、予め定められた手順を踏めば、パケット廃棄や遅延等の品質劣化無く、転送データを送信先まで転送することが可能であるとする。この無線LAN上では、データは図38のように、イーサネットフレームと同様のフォーマット、すなわち「送信元アドレス、宛先アドレス、データ」のようなフォーマットを持つ、無線フレームで転送される。

【0129】さて、IEEE1394バスの同期チャネル#xを通して受信したデータを、無線ノード側にフォワードすべく、無線区間のQOS設定を行う。さらにISO信号送受信部2203（同期チャネル#xを受信）と無線ISO信号送受信部2206（QOS保証を行なう無線フレームにて送信）を図22の点線のように接続し（まだ暗号の復号化ができないため）、1394インタフェース2201から入力されたISO入力データを無線区間にそのままフォワードできるようにしてもよい（ステップS2504，S2706，S2707）。

【0130】さらに、無線ノード2103に対して、「上記無線フレームを通して、データを送信するので、これを受信し、その結果をディスプレイに表示せよ」との命令を無線ノード制御パケットの形で送信する（ステップS2505，S2708，S2802）。この制御プロトコルには、IEEE1394AV／Cプロトコル、あるいはIEC61883プロトコルや、これらを変形したものを用いてもよい。後述するように、本実施形態では、無線LAN上に同期チャネルの概念はないものの、転送するデータにソースID（SID）なる領域を設け、無線区間にQOSデータを送信しているノード毎に、転送しているQOSデータを一意に区別できるようになっており、このSIDの値をIEEE1394の同期チャネルのように、データフローの判別に用いることができる。無線ノード制御パケットの一例を図39に示す。パケットの送信元は中継ノード2102である。

【0131】これを受信した無線ノード2103は、αなるSIDが付与されて、データがQOS転送されてくることを認識する。

【0132】この後、送信ノード2101は、同期チャネル#xを通して、暗号化されたMPEG映像を転送する（ステップS2506，S2603）。コンテンツ鍵はK1とする。この暗号鍵は、後述する交換鍵やシードの関数として導出される。

【0133】また、この暗号化されたMPEG映像を送信するフレームには、同期チャネル番号の他、送信ノー

ドを識別する「送信ノードＩＤ」が含まれていてもよい。

【０１３４】これを受信した中継ノード２１０２は、データが暗号化されていることを認識するとともに、例えば受信データに含まれる「送信ノードＩＤ」を参照して、このデータを送信しているのが送信ノード２１０１であることを認識し（ステップＳ２７０９）、送信ノード２１０１に対して、「同期チャネル＃ｘを通して、このデータを送出しているのは、送信ノード２１０１のどのサブユニットか」を確かめるため、認証先の問合せを行なう（ステップＳ２５０７，Ｓ２７１０）。この際、データが転送されている同期チャネル番号（＃ｘ）を記載して、送信ノード２１０１が、データを送信しているサブユニットを特定できるようにしておくとともに、このデータを受信する自身のサブユニット（本実施形態の場合、中継ノード２１０２のＭＰＥＧデコード／ディスプレイサブユニットのサブユニットＩＤ＝０）も通知する。これは、送信ノード２１０１から見た認証先を通知する役割を持つ。

【０１３５】なお、この認証先問合せパケットと、後述する認証先応答パケットは、認証機関のプライベート鍵でハッシュや暗号化したデータを電子署名として記載しておき、改ざん等が無いことを確認できるようにしてもよい。

【０１３６】さて、認証先問合せを受信（ステップＳ２６０４）した送信ノード２１０１は、同期チャネル＃ｘに対して送信しているデータを受信しているサブユニットが、中継ノード２１０２のＭＰＥＧデコード／ディスプレイサブユニットであることを認識するとともに、自らが該同期チャネル＃ｘに送信しているサブユニットが、映像送信サブユニット（サブユニットＩＤ＝０）であることを、認証先応答パケットとして、中継ノード２１０２に通知する（ステップＳ２５０８，Ｓ２６０５）。

【０１３７】これにより、中継ノード２１０２は、同期チャネル＃ｘにデータを送信しているサブユニットが、送信ノード２１０１の映像送信サブユニット（サブユニットＩＤ＝０）であることを認識できる（ステップＳ２７１１）。

【０１３８】同期チャネル＃ｘにデータを送信しているサブユニットが、送信ノード２１０１の映像送信サブユニットであることを認識した中継ノード２１０２（のＭＰＥＧデコード／ディスプレイサブユニットの代理機能）は、続いて送信ノード２１０１の映像送信サブユニットに対して認証要求を行なう。この認証要求には、中継ノード、あるいは中継ノードのＭＰＥＧデコード／ディスプレイサブユニットの認証フォーマット（Ｂｃｅｒｔ）が共に転送される（ステップＳ２５０９，Ｓ２６０６，Ｓ２６０７，Ｓ２７１２）。この認証要求と認証フォーマットの交換は、第１の実施形態と同様に、送信ノード２１０１（の映像送信サブユニット）から中継ノード２１０２（のＭＰＥＧデコード／ディスプレイサブユニット）に向けても行われる（ステップＳ２５１０，Ｓ２６０８，Ｓ２７１３，Ｓ２７１４）。このように、第２の実施形態においても、認証・鍵交換にサブユニットに関する情報も交換するのは、同じ装置同士の通信でも、通信しているサブユニットが異なれば、異なる鍵の使用ができるようにするためである。

【０１３９】お互いに認証が完了した両ノードは、第１の実施形態と同様に認証・鍵交換手続きを行い（ステップＳ２５１１１，Ｓ２５１１２，Ｓ２６０９，Ｓ２７１５）、認証鍵Ｋａｕｔｈ１を共有する。この認証鍵を使って、送信ノード２１０１は、交換鍵やシードの転送を中継ノード２１０２に対して行ない（ステップＳ２５１２，Ｓ２６１０，，Ｓ２７１６）、結局、中継ノード２１０２では、コンテンツ鍵Ｋ１の値を知ることができるようになる（ステップＳ２７１７）。

【０１４０】以降、転送されてくるコンテンツ鍵Ｋ１で暗号化されたＭＰＥＧ映像（同期チャネル＃ｘ経由）（ステップＳ２５１３，Ｓ２６１１，Ｓ２６１２）は、中継ノード２１０２にて復号化され（ステップＳ２５１４，Ｓ２７１８）、さらに無線区間用に別に用意されたコンテンツ鍵ｋ２で再暗号化され（ステップＳ２５１５，Ｓ２５１６，Ｓ２７１９）、無線区間上をＱＯＳが保証される形で、無線ノード２１０３に対して送信される（ステップＳ２５１７，Ｓ２７２０，Ｓ２８０３）。この時点では、ＭＰＥＧ映像はＩＳＯ信号送受信部２２０３、暗号復号化部２２０４、暗号化部２２０５、無線ＩＳＯ信号送受信部２２０６というパスを通る。

【０１４１】先に述べたように、このとき中継ノード２１０２が、無線区間側に送信しているデータの区別ができるようにするために、ソースＩＤなる、中継ノード２１０２で一意な値を付与して送出してもよい。ここでは、この一意な値をαとする。すなわち、αの値のついたデータは、ＩＥＥＥ１３９４の同期チャネル＃ｘから受信したデータ（をコンテンツ鍵Ｋ１で復号化し、コンテンツ鍵Ｋ２で再暗号化したもの）である。中継ノード２１０２は、αのＳＩＤを付けて無線区間に送出しているデータは、自身の無線区間側の映像送信サブユニットの代理機能から送信しているデータであることを認識している。

【０１４２】これを受信した無線ノード２１０３の動作は、基本的に先に説明した、暗号化データを受信した中継ノード２１０２の動作と同様である。すなわち、データが暗号化されていることを認識するとともに、例えば受信データに含まれる「送信元アドレス」を参照して、このデータを送信しているのが中継ノード２１０２であることを認識し、中継ノード２１０２に対して、「αなる値を付与して、このデータを送出しているのは、中継ノード２１０２のどのサブユニットか」を確かめるた

め、中継ノードに認証先の問合せを行なう（ステップS2518，S2804）。

【0143】この際、データが転送されているSIDの値（α）を記載して、中継ノード2102が、データを送信しているサブユニットを特定できるようにしておくとともに、このデータを受信する受信側のサブユニット（本実施形態の場合、無線ノード2103のMPEGデコード／ディスプレイサブユニットのサブユニットID＝0）も通知する。これは、中継ノード2102から見た認証先を通知する役割を持つ。

【0144】認証先問合せを受信（ステップS2721）した中継ノード2102は、SID＝αに対して送信しているデータを受信しているサブユニットが、無線ノード2103のMPEGデコード／ディスプレイサブユニット（サブユニットID＝0）であることを認識するとともに、自らがSID＝αを付与して送信しているサブユニットが、映像送信サブユニットであることを、認証先応答パケットとして、無線ノード2103に通知する（ステップS2519，S2722，S2805）。

【0145】これにより、無線ノード2103は、SID＝αを付与してデータを送信しているサブユニットが、中継ノード2102の映像送信サブユニットであることを認識できる。

【0146】SID＝αを付与してデータを送信しているサブユニットが、中継ノード2102の映像送信サブユニットであることを認識した無線ノード2103（のMPEGデコード／ディスプレイサブユニット）は、続いて中継ノード2102の映像送信サブユニットに対して認証要求を行なう（ステップS2520，S2723，S2724，S2806）。この認証要求には、無線ノード（または無線ノードのMPEGデコード／ディスプレイサブユニット）の認証フォーマット（Dcert）が共に転送される。この認証要求と認証フォーマットの交換は、中継ノード2102（の映像送信サブユニット）から無線ノード2103（のMPEGデコード／ディスプレイサブユニット）に向けても行われる（ステップS2521，S2725，S2807）。

【0147】お互いに認証が完了した両ノードは、続いて認証・鍵交換手続きを行い（ステップS2522，S2523，S2726，S2808）、認証鍵Kauth2を共有する。この認証鍵を使って、中継ノード2102は、交換鍵やシードの転送を無線ノード2103に対して行い（ステップS2524，S2727，S2809）、結局、無線ノード2103で、コンテンツ鍵K2の値を知ることができるようになる（ステップS2810）。

【0148】なお、これまでの説明では送信ノードと中継ノード間の認証・鍵交換と、中継ノードと無線ノード間の認証・鍵交換とは、順次行われる形で説明したが、逆の順番でもよいし、両者を並行して行うことも可能である。

【0149】以降、転送されてくるコンテンツ鍵K1で暗号化されたMPEG映像（ステップS2525）は、中継ノード2102にて復号化され（ステップS2526）、さらに無線区間用に別に用意されたコンテンツ鍵K2で再暗号化され（ステップS2527，S2528，S2728）、無線区間上をQOSが保証される形で、SID＝αが付与された無線フレームの形で無線ノード2103に対して送信される（ステップS2529，S2729）。

【0150】今度は、無線ノード2103は、先に入手した交換鍵、シードの値を使って、コンテンツ鍵K2を計算できるので、これを復号化することが可能であり（ステップS2530，S2811）、これをディスプレイ部2307にて再生する（ステップS2812）。

【0151】このように、IEEE1394バスと無線網のと間に代理ノードが存在するような相互接続の環境においても、代理機能を提供する中継ノードと送信ノード、および中継ノードと受信ノードが、それぞれの区間で、認証手続きや鍵交換手続きを行うことで、実際のMPEG映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。これによって、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送が可能になる。

【0152】もちろん、中継ノード2102の「生のMPEGデータ」が流れる部分、具体的には暗号復号化部2204と暗号化部2205との間には、データをコピーされる危険が考えられるため、この部分でデータコピーがなされないようにするための工夫（例えば、暗号復号化部と暗号化部を一体のLSIにするなど）がなされていると、この間でプローブをあてるなどしてデータを盗聴（不正コピー）することが実質的に不可能になるため、このような対策を行っておくことが有益である。

【0153】（第3の実施形態）次に、第3の実施形態について説明する。

【0154】第3の実施形態では、IEEE1394上において、HAVi規格（Specification of the Home Audio/Vidio Interoperability（HAVi） Architecture）等に代表される、AV/Cの上位レイヤに相当するAV機器制御ソフトウェアが稼働している場合における実施形態である。

【0155】図40に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第1の実施形態と同様である。

【0156】図41に、送信ノード4101の内部構造の一例を示す。これも第1の実施形態の場合とほぼ同様

であるが、IEEE1212レジスタ4407を強調のため、追加記述している。IEEE1212レジスタ4407には、送信ノード4101の属性、例えば「どのベンダの製品かを示す情報、例えばVTRやチューナ等といったどのようなジャンルの製品かを示す情報、製造番号、制御ソフトウェアの配置URL、制御アイコン、コマンド一覧」等の情報が含まれる。

【0157】次に、図42に、中継ノード4102の内部構造の一例を示す。中継ノード4102も、第1の実施形態とほぼ同様の構成であるが、本実施形態のシーケンスを説明する際に必要なIEEE1212レジスタ4213を1394バス構成認識部4206内に特に記した点と、HAVi処理部4212を持つ点が第1の実施形態と異なる。HAVi処理部4212には、いわゆるHAViバイトコードの処理を行う仮想マシン（VM）が存在する。また、本実施形態においては、制御画面の記述を行う「パネルサブユニット」の代理機能を代理サブユニット構成部4207が持つ。

【0158】次に、図43に、無線ノード4103の内部構造の一例を示す。これについても、第1の実施形態の場合と基本的には同様である。

【0159】次に、HAVi環境における、実際のコピープロテクションを施した上でのMPEG映像全体のシーケンスについて、図44／図45（全体のシーケンス例）、図46／図47（送信ノード4101のフローチャート例）、図48／図49／図50（中継ノード4102のフローチャート例）、図51／図52（無線ノード4103のフローチャート例）を参照しながら説明する。

【0160】まず、無線ノード4103は、自分の構成情報を中継ノード4102に通知する（ステップS4501）。このとき、これらの構成情報は、IEEE1212レジスタ形式の情報として中継ノード4101に送付するものとする。すなわち、中継ノード4102が、無線ノード4103に対して「IEEE1212で規定されるCSR（コマンド・ステータスレジスタ）空間の、このアドレスに相当する部分についての情報」を要求し、これに無線ノード4103が答える形でこのやり取りが行われてもよい。ここで、前述のように、この構成情報には、自分（無線ノード）がMPEGデコード／ディスプレイ機能を持つといったことや、認証のための認証フォーマットを持っていること、等が含まれる。ここで、無線ノード4103が持っている認証フォーマットをBcertとする。

【0161】これを受信した中継ノード4102は、無線ノード4101が認証フォーマットを持つことや、MPEGデコード／ディスプレイ機能を持っていることを確認する（ステップS4701）。中継ノード4102は、無線ノード4101がMPEGデコード／ディスプレイ機能を持っていることをIEEE1394バス側のノードに対して知らせるため、このMPEGデコード／ディスプレイ機能を、中継ノード4102自身のサブユニットとしてIEEE1394バス側に広告する（ステップS4502）。具体的には、自身のIEEE1212レジスタに「自分はMPEGデコード／ディスプレイ機能を持っている」旨を記載したり、AV／Cプロトコルでサブユニット機能の問い合わせを受けた場合に、自分がMPEGデコード／ディスプレイサブユニットを持っているという形で応答を返したりする（これにより、送信ノード4101等のIEEE1394に接続されたノードは、中継ノードにこの機能が存在すると認識することになる）。

【0162】そのために、中継ノード4102は、代理テーブル4208を持つ。代理テーブル4208は、図53／図54のように、中継ノード4102が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【0163】ここでは、図53のように、無線ノード4103のMPEGデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップS4702，S4703）。

【0164】以上と逆の手続きがIEEE1394バス4104上の送信ノード4101の代理登録を無線区間側に対してみせる形で行われる（ステップS4503，S4504）。すなわち、送信ノード4101のIEEE1212レジスタ4407に、自分が映像送信機能を持つこと、およびパネル機能（制御画面機能）を持つことを記述しておき、これを中継ノード4102が読み込む（ステップS4601，S4704）。この送信ノード4101の機能を、中継ノード4102の機能として、代理して無線区間側のIEEE1212相当機能（無線区間側のCSR空間）に反映し、無線ノード4103側には、上記映像送信機能、およびパネル機能が中継ノード4102の機能であるものとして認識してもらう。この対応関係を、代理テーブル4208に図54のように反映する（ステップS4705）。

【0165】このようにして代理テーブル4208は、図53／図54のように構成される。また、送信ノード4101から見た中継ノード4102の内部構造を図55に、無線ノード4103から見た中継ノード4102の内部構造を図56に、それぞれ示す。

【0166】なお、この時点で、ステップS4503の送信ノード構成情報の中に、送信ノード4101を制御するためのHAViのバイトコードが含まれており、中継ノード4102は送信ノード4101の代理サーバ、すなわちDCM（デバイスコントロールモジュール）の機能を有していてもよい。この場合、このバイトコードは、中継ノード4102のHAVi処理部4212内の仮想マシン上で稼働することになる。

【0167】さて、中継ノード4102にパネル機能が

あるものと認識した無線ノード４１０３は、中継ノード４１０２の（パネルサブユニット）に対して、パネルの表示要求のコマンドを送出する（ステップＳ４５０５，Ｓ４８０２）。これを受信（ステップＳ４７０６）した中継ノード４１０２は、代理テーブル４２０８を参照し、このパネル機能の実体が送信ノード４１０１に存在していることを認識し、前記パネル表示要求コマンドを送信ノード４１０１に対してフォワードする（ステップＳ４５０６，Ｓ４７０７）。

【０１６８】これを受信（ステップＳ４６０１）した送信ノード４１０１は、ＡＶ／Ｃプロトコルにてパネル応答（つまり、制御画面の送信）を行う。送信先は、中継ノード４１０２である（ステップＳ４６０３，Ｓ４５０７）。これを受信（ステップＳ４７０８）した中継ノード４１０２は、代理テーブル４２０８を参照して、これを無線ノード４１０３にフォワードする（ステップＳ４７０９，Ｓ４５０８，Ｓ４８０３）。

【０１６９】ここで、図５７に、無線ノード４１０３に送られてきた制御画面の一例を示す。この制御画面（パネル）では、６つの映画のタイトルを表示したボタンが提供される。これらのボタンは、例えば「ボタン１」、「ボタン２」、…等の名前が付けられており、ユーザがあるボタンを押すと、例えば「ボタン１が押されました」というコマンドの形で、パネルの送信元に送られる仕組みとなっているものとする。

【０１７０】さて、無線ノード４１０３は、中継ノード４１０２が提供していると認識している映像送信サービスを受けようと考え（実際に提供しているのは送信ノード４１０１）、無線ノード制御パケットを使って（ステップＳ４５０９）、映像を流すための無線同期チャネル＃ｙを確保し、このチャネルを中継ノード４１０２の映像送信サブユニットに接続するためのコマンドを中継ノード４１０２に対して発行する（ステップＳ４８０４）。これを受信した中継ノード４１０２は、代理テーブル４２０８を参照して、実際にこのＡＶ／Ｃコマンドが発行されるべきノード（送信ノード４１９１）を確認し、ＩＥＥＥ１３９４バス上に必要な帯域を確保するとともに（同期チャネル＃ｘ）、内部のＩＳＯ信号送受信部４２０４を設定して、ＩＥＥＥ１３９４バスの同期チャネル＃ｘと無線同期チャネル＃ｙとを相互に接続する（ステップＳ４７１０，Ｓ４７１１，Ｓ４７１２，Ｓ４５１０）。また、中継ノード４１０２は、送信ノード４１０１に対し、同期チャネル＃ｘを映像送信サブユニットに接続するコマンドを発行する（ステップＳ４５１１，Ｓ４７１３）。これを受信（ステップＳ４６０４）した送信ノード４１０１は、映像送信サブユニットの実体である内部の映像ストリームの流れるパス（図４１で２重矢印になっている部分）をＩＥＥＥ１３９４バスの同期チャネル＃ｘに接続する。

【０１７１】これと前後して、無線ノード４１０３のユーザは、見たい映像を選択するために図５７のパネルの中から適当な番組を選択すべく、制御画面のボタンを押す（例えば、マウスを使ってクリックする、ペン入力する、タッチする、など）。この操作は、中継ノード４１０２に伝達され、これは代理テーブル４２０８の参照を経て送信ノード４１０１へのコマンドに変換される（ステップＳ４８０５，Ｓ４７１４，Ｓ４７１５，Ｓ４６０５，Ｓ４５１２，Ｓ４５１３）。

【０１７２】この後、送信ノード４１０１は、同期チャネル＃ｘを通して、暗号化されたＭＰＥＧ映像を転送する（ステップＳ４５１４，Ｓ４６０６）。これは、中継ノード４１０２にて中継され、無線ノード４１０３に到達する（ステップＳ４７１６）。

【０１７３】後の手続きは、第１の実施形態の場合と同様であり、暗号化されたＭＰＥＧ映像が無線ノード４１０３に到達する（ステップＳ４８０６）が、この時点で無線ノード４１０３はこの暗号を解くための鍵を有していないため、ＭＰＥＧ映像の送信元と認証手続きを開始する。認証手続き以降の手続きについては第１の実施形態と同様であるので、ここでの詳細な説明は省略する。

【０１７４】なお、第１の実施形態に従えば、認証は送信ノード４１０１の映像送信サブユニットに相当する機能と、無線ノードの映像受信サブユニットに相当する機能ととの間で行われると考えられるが、第３の実施形態の場合には、このような認証方式の他に、送信ノード４１０１のパネルサブユニットが認証の対象となるような方式も考えられる。この場合は、送信ノード４１０１のパネルにデバイスＩＤが割り当てられることになる。

【０１７５】なお、ＨＡＶｉにおいては、送信ノード４１０１から送られてくるバイトコードであるＤＣＭ等の中に、送信ノード４１０１を制御するための制御画面情報が含まれる場合がある。このようなモジュールをＤＤＩ（データドリブンインタラクション）と呼ぶ。このようなモジュールは、例えば中継ノード４１０２内のＨＡＶｉ処理部４２１２にて展開され、制御画面が生成される。本実施形態では、この制御画面（あるいは、それと同等の機能を持つ制御画面）を無線ノード側に見せることを考える必要があるが、この場合は、代理サブユニット構成部４２０７が、このＤＤＩに含まれる画面構成情報を認識して（例えば、画面構成のためのシステムコールをイベントして認知して、生成される最終画面の概要を推察する方法や、完成した制御画面をもとにする方法等が考えられる）、パネルとしてこの制御画面を再構成し、無線区間に「パネルサブユニット」としてこれを公開する方法が考えられる。この場合には、代理テーブル４２０８には、このパネルと、ＤＤＩで生成されるべきＨＡＶｉやＡＶ／Ｃのコマンド（中継ノード４１０２から送信ノード４１０１に対して発行される）の対応テーブルが用意されることになる。この方法は、無線ノード４１０３内にＨＡＶｉバイトコードの仮想マシンが存在

しなくても有効であるため、HAVi仮想マシンを持たない無線ノード4103から、HAVi機器の制御を可能とする方法である。

【0176】（第4の実施形態）次に、第4の実施形態について説明する。

【0177】図58に、本実施形態の全体構成の一例を示す。

【0178】図58に示されるように、第4の実施形態では、ある家庭のホームネットワークであるIEEE1394バス6104と、公衆網（ここでは、一例としてインターネットとするが、電話網等でもよい）6105とが、ホームゲートウェイ6102で接続され、送信ノード6101と受信ノード6103との間で、認証手続き、暗号化の手続きを経た上で例えば映像データのやり取りを行う。ここで、インターネット6105（のアクセス網部分）は、IEEE1394バス6104と比べて通信帯域が非常に細く、IEEE1394バスでやり取りされる映像情報（一例としてMPEG2映像であるとする）は、帯域が足りずに通せないため、ホームゲートウェイ6102においてトランスコーディング、つまりMPEG2符号からMPEG4符号への符号変換を行った上で、伝送を行うことを考える。

【0179】第4の実施形態においても、第2の実施形態と同様に、ホームゲートウェイにて、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りを終端する。すなわち、送信ノードとホームゲートウェイ、ホームゲートウェイト受信ノードとで、おのおのコピープロテクション手続きは閉じている。この実施形態においても、ホームゲートウェイは、送信ノードや受信ノードに対して代理サービスを提供し、また、コピープロテクションについては、ホームゲートウェイ自身が認証フォーマットを持ち、ホームゲートウェイ自身が1394バス区間および無線区間のMPEGデータの暗号化転送についてのそれぞれの責任を終端する。

【0180】次に、図59に、送信ノード6101の内部構造の一例を示す。これは基本的にはこれまでの実施形態と同様の構成である。

【0181】次に、図60に、ホームゲートウェイ6102の内部構造の一例を示す。

【0182】ホームゲートウェイ6102の基本的な構成は、無線インタフェースではなくインターネットインタフェース6202を有している点、代理サブユニット構成部ではなく代理ホームページ作成部6210を有している点、ホームページの作成・蓄積部6211を有している点、暗号復号化部6204と暗号化部6205との間にMPEG2／MPEG4変換部6214を有している点を除くと、第2の実施形態の中継ノードの構成とほぼ同様である。上記の相違点については順次説明していく。

【0183】ホームゲートウェイ6102は、インターネット側のノードに対してIEEE1394バス側のノード（本実施形態では、送信ノード2101）の代理サーバとなり、IEEE1394バス側のノードの機能を代理で提供する機能を持つ。送信ノード6101が提供しているサービス（本実施形態の場合、映像送信サービス）には、ホームゲートウェイ6102が提供しているホームページを介してアクセスすることが可能である。ここで、受信ノード6103からは、送信ノード6101のサービスは、ホームゲートウェイ6102のホームページを介して見えるため、これをホームゲートウェイ6102が提供するIP（インターネット）上のサービスとして解釈されてもよい。

【0184】また、ホームゲートウェイ6102は、第2の実施形態と同様に、IEEE1394バス側から受信したデータ（MPEG2映像データ）をインターネット側にフォワードする機能を持つが、認証やデータの暗号化等、コピープロテクションに関する手続きがIEEE1394バス区間とインターネット区間との両方について、このホームゲートウェイ6102において終端されている。IEEE1394バス側については、認証フォーマットBcertをIEEE1394コピープロテクション処理部6208に、インターネット区間側については、認証フォーマットCcertをインターネット側コピープロテクション処理部6212にそれぞれ持ち、IEEE1394バスの同期チャネルから入力されてきた暗号化データについては、ISO信号送受信部6203にて受信→暗号復号化部2204にて暗号復号化→復号化されたMPEG2映像をMPEG2／MPEG4変換部6214にてトランスコード→MPEG4映像を暗号化部6205にて再暗号化→AV信号送受信部6206にてインターネット側に送信、というプロセスを踏む。

【0185】ここで、AcertとBcertは、同じ認証機関（例えばIEEE1394のコピープロテクションを担当する認証機関）が発行した認証フォーマットであると仮定するが、後述するインターネット区間の認証フォーマット（後述するCcertとDcert）については、同じくこの認証機関が発行したものであってもよいし、インターネット区間を担当する別の認証機関が発行する認証フォーマットであってもよい。

【0186】なお、本実施形態においては、認証フォーマット（Acert～Dcert）は、ノード（あるいはネットワークインタフェース）毎に1つ持つのではなく、サブユニット毎（サブユニット種別毎）、あるいはインターネットアプリケーション毎に1つ持ってもよい。すなわち、異なるインターネットアプリケーションでは、異なる認証フォーマットを用いてもよい。ここで、フローとは、インターネットの（送信アドレス、送信ポート、受信アドレス、受信ポート）の組で表現され

る一連のデータ流を指す。

【0187】次に、図61に、受信ノード6103の内部構造の一例を示す。

【0188】コピープロテクション処理部6303がインターネット向けの認証フォーマットDcertを持っている。第2の実施形態との相違点は、インタフェース（インターネットインタフェース6301、制御パケット送受信部6302、AV信号送受信部6304）がインターネット対応となっている点である。ここで、制御パケット送受信部6302はTCP、AV信号送受信部6394はUDPのトランスポートプロトコルを持つパケットの送受信モジュールであってもよい。

【0189】次に、実際のコピープロテクションを施した上での映像送信全体のシーケンスについて、図62／図63（全体のシーケンス例）、図64／図65（送信ノード6103のフローチャート例）、図66／図67／図68／図69（ホームゲートウェイ6102のフローチャート例）、図70／図71（受信ノード6103のフローチャート例）を参照しながら説明する。

【0190】まず、ホームゲートウェイ6102は、送信ノード6101のIEEE1212レジスタの読み込みなどを通して、送信ノードについての属性や構成情報を収集する（ステップS6501，S6601，S6701，S6502，S6602，S6702）。これを通して、ホームゲートウェイ6102は、送信ノード6101が映像送信機能を持つこと、パネル機能を持つこと、認証フォーマットを持っていること等を把握する。

【0191】これを受けて、ホームゲートウェイ6102は、送信ノード6101を遠隔制御するためのホームページを作成する（ステップS6503）。基本的には、送信ノード6101が持つパネルと同様の画面を「送信ノード制御用ホームページ」として作成する。ホームページ上に配置された制御用のボタン等は、それぞれ送信ノード6101のパネルサブユニットのボタンに対応する等して、代理ホームページ作成部6210内の変換テーブルに対応の一覧が記述される。例えば、送信ノード6101のパネルサブユニットに「再生」とかかれているボタンが存在する場合には、該ホームページにも「再生」とかかれているボタンを用意して、この関係を前記変換テーブルに記述しておく。もし、このホームページのユーザがこのボタンを押した場合には、ホームゲートウェイ6102から送信ノード6101のパネルサブユニットの「再生」ボタンに対して「ボタンが押された」というインタラクションが返る形となる。図72（a）に送信ノード6101のパネルサブユニットの持つパネルの一例を、図72（b）にホームゲートウェイ6102の作成した送信ノード制御用ホームページの一例をそれぞれ示す。

【0192】さて、インターネット上の受信ノード6103は、インターネットを介してこのホームゲートウェイ6201にアクセスし、送信ノード6101の制御画面を含むホームページを要求し、このホームページが送付される（ステップS6504，S6801，S6703）。これを見て、受信ノード6103のユーザは、画面上の映像送信を要求するボタン（例えば、図72（b）の「再生」ボタン）を押したものとする。この結果、例えば「再生ボタンが押された」、というインタラクションが、インターネット経由でホームゲートウェイにHTTPを通じて通知される（ステップS6505，S6802，S6704）。

【0193】この通知と前後して、ホームゲートウエイ6102と受信ノード6103との間で、やり取りされるストリームが転送されるIPフロー、すなわち（送信IPアドレス、送信ポート、受信IPアドレス、受信ポート）の組の決定や、セッション制御（符号化方式や認証方式等）のネゴシエーション等が行なわれる（ステップS6505，S6705，S6803）。例えば、RTSP（リアルタイムトランスポートストリーミングプロトコル）やSDP（セッションデスクリプションプロトコル）等を用いて、符号化方式や認証の方式、ポートの番号の決定などが行われる。

【0194】ホームゲートウエイ6102は、これらの処理を受け、映像送信を行なう実体は、送信ノード6101の映像送信サブユニットであることを認識し、送信ノード6101に対してAV／Cプロトコル等で、データ転送のための同期チャネル#xの設定や、映像送信サブユニットに対して、映像送信の要求などのコマンドを発行する（ステップS6506）。

【0195】これを受けて、送信ノード6101から同期チャネル#xを通して、暗号化されたMPEG映像がホームゲートウエイ6102に対して送出される（ステップS6507，S6603，S6604）。その後は、第2の実施形態のIEEE1394側の手順と同様の手順で、認証先問合せ／応答、認証要求、認証・鍵交換手続き、交換鍵／シード転送等が行われ、ホームゲートウエイ6102にてコンテンツ鍵K1の計算ができるようになる（ステップS6508～S6514，S6605～S6611，S6706～S6715）。

【0196】以降、同期チャネル#xを通して暗号化されたMPEG映像（ステップS6515，S6612，S6613）を受信したホームゲートウエイ6102は、暗号復号化部6204にて、これをコンテンツ鍵K1を用いてMPEG2映像に復号化する（ステップS6516，S6517，S6716）。次に、抽出したMPEG2映像を、MPEG2／MPEG4変換部6214でMPEG4映像にトランスコードする（ステップS6518）。このMPEG4映像を、コンテンツ鍵K2を用いて、暗号化部6205で再暗号化し（ステップS6519，S6520，S6717，S6718）、これをIPパケット化する。その場合、先のセッション制

御の手順で決めたように、送信ＩＰアドレスはＣ（ホームゲートウエイのＩＰアドレス）、送信ポート番号はｃ、受信ＩＰアドレスはＤ（受信ノードのＩＰアドレス）、受信ポート番号はｄであるようなＩＰパケットを生成する（ステップＳ６５２１，Ｓ６７１９）。

【０１９７】これを受信した受信ノード６１０３は、受信したデータが暗号化されていることを認識する（ステップＳ６８０４）。受信ノード６１０３は、このデータを送信しているのは、到着したパケットのＩＰヘッダを参照すること等により、ホームゲートウエイ６１０２であることを認識し、ホームゲートウエイ６１０２に対して、認証要求を送信する（ステップＳ６５２２，Ｓ６８０５）。この認証要求のパケットもＩＰパケットでもよい。認証要求のためのポート番号は、認証を行なう手続きに予め割当てられている番号を用いてもよい。この際、この認証要求のパケットに、ストリーム転送のフローＩＤ（Ｃ、ｃ、Ｄ、ｄ）を付与して転送する。このことにより、ホームゲートウエイ６１０２は、どのフローに対する認証要求であるかを認識することができる。図示はしていないが、この認証要求には、受信ノードの（本ストリーム用の）認証フォーマット等も含まれている。

【０１９８】また、トランスポートプロトコルとしてＲＴＰ（Ｒｅａｌｔｉｍｅ Ｔｒａｎｓｐｏｒｔ Ｐｒｏｔｏｃｏｌ）を用いていること等を同時に伝えてもよい。

【０１９９】これを受けてホームゲートウエイ６１０２は、フロー（Ｃ、ｃ、Ｄ、ｄ）のための認証要求であることを認識し、このフローのための認証フォーマットを含んだ認証要求を、受信ノード宛てに送り返す（ステップＳ６５２３，Ｓ６７２０～Ｓ６７２２，Ｓ６８０６，Ｓ６８０７）。このとき、この認証要求には前記フローＩＤ等が含まれる。

【０２００】次に、両者は、認証・鍵交換手続き、交換鍵／シードの転送等を、ＩＰパケット上で行う（ステップＳ６５２４～Ｓ６５２６，Ｓ６７２３，Ｓ６７２４，Ｓ６８０８～Ｓ６８１０）。これにより、受信ノード６１０３は、コンテンツ鍵Ｋ２の生成が行なえるようになっている。

【０２０１】よって、以降、コンテンツ鍵Ｋ２にて暗号化された、フロー（Ｃ、ｃ、Ｄ、ｄ）を通して送られてくるＭＰＥＧ４データ（ステップＳ６５２７～Ｓ６５３３，Ｓ６７２５，Ｓ６７２６，Ｓ６８１１）は、上記のように用意されたコンテンツ鍵ｋ２にて復号化することが可能となる（ステップＳ６５３４）。復号化されたＭＰＥＧ４データは、ＭＰＥＧデコード部６３０６にて復号化され（ステップＳ６８１２）、これをディスプレイ部６３０７にて再生する（ステップＳ６８１３）。

【０２０２】このように、家庭網とインターネットが相互接続された環境においても、代理機能を提供するホームゲートウェイと送信ノード、およびホームゲートウェイと受信ノードが認証手続きや鍵交換手続きを行うことで、実際のＭＰＥＧ映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。このように、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【０２０３】第２の実施形態と同様に、ホームゲートウェイ６１０２において、「生のＭＰＥＧデータ」が流れる部分、具体的には暗号復号化部６２０４、ＭＰＥＧ２／ＭＰＥＧ４変換部６２１４、暗号化部６２０５との間は、データコピーがなされないようにするための工夫、例えば一体のＬＳＩに封止する等の対策を立てておいてもよい。

【０２０４】（第５の実施形態）次に、第５の実施形態について説明する。

【０２０５】第４の実施形態が、公衆網（インターネット）を介して家庭網にアクセスし、コピープロテクションを考慮した上で家庭網上の端末とインターネット上の端末間でコンテンツをやり取りする場合であったのに対し、第５の実施形態は、公衆網を介して家庭網間でコンテンツをやり取りする場合である。

【０２０６】図７３に、本実施形態の全体構成図を示す。

【０２０７】図７３に示されるように、第５の実施形態では、２つの家庭網８１０５，８１０７が公衆網（ここでは、一例としてインターネットとするが、Ｂ－ＩＳＤＮ等でもよい）８１０６にて接続されている。第１の家庭網８１０５上の送信ノード８１０１から、コピープロテクションを考慮した形で、ＡＶコンテンツを第２の家庭網８１０７上の受信ノード８１０４に送信する。ここで、第４の実施形態では、公衆網部分の通信帯域が非常に細い場合の例を示したが、本実施形態では、公衆網の通信帯域は十分な容量を持つものとする。

【０２０８】第５の実施形態においては、第１の実施形態の中継ノードと同様に、ホームゲートウェイ８１０２，８１０３にて、ＩＥＥＥ１３９４バス８１０５，８１０７上のサービスを公衆網側に代理サービスする。すなわち、インターネット上からは、インターネットのサービスとして、家庭網上の装置やサービス、コンテンツが見える。また、ホームゲートウェイ８１０２，８１０３は、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りについてはこれらをフォワードする。

【０２０９】送信ノード８１０１や受信ノード８１０４は、基本的には第４の実施形態と同様の構成である。

【０２１０】図７４に、ホームゲートウェイ８１０２，８１０３の内部構造の一例を示す。

【０２１１】ホームゲートウェイ８１０２の基本的な構

成は、コピープロテクションを終端しない点（これは、第1の実施形態の中継ノードと同様）、および暗号の符号化・復号化・符号変換を行わない点（これも、第1の実施形態の中継ノードと同様）を除き、第4の実施形態のホームゲートウェイの構成とほぼ同様である。

【0212】図75に、全体のシーケンスの一例を示す。

【0213】ここでは、第2の家庭網8107のユーザが、ホームゲートウェイ8103の制御画面を使って、送信ノード8101のコンテンツを、インターネット8106を介して受信ノード8104に配信させる場合を考える。

【0214】まず、第4の実施形態と同様に、ステップS8301の構成認識と、ステップS8302の送信ノード制御用ホームページ作成が行われる。

【0215】第2の家庭網8107のユーザは、ホームゲートウェイ8103を操作し、ホームゲートウェイ8102から送信ノード制御用のホームページ（制御画面）を持ってくる（ステップS8303）。また、例えば図76に例示するような受信ノード8104の制御画面も同時に開く。そこで、図76のように、送信ノード内のコンテンツ一覧から、適当なものを例えばドラッグアンドドロップするなどして、ホームゲートウェイ8103に映像配信を命令する（ステップS8304）。

【0216】すると、第4の実施形態と同様に、映像送信要求がホームゲートウェイ8102に（インターネットコマンドとして）発行され（ステップS8305）、これがホームゲートウェイ8102にてAV/Cプロトコルコマンドに翻訳され、送信ノード8101から受信ノード8104間の通信パス（IEEE1394バス8105上の同期チャネル#x、インターネット上のコネクション、IEEE1394バス上の同期チャネル#y）が設定される（ステップS8306，S8307）。この上を、暗号鍵Kで暗号化されたMPEG2映像が配信される（ステップS8308～S8310）。

【0217】第1の実施形態と同様に、これを受信した受信ノード8106は、送信元に認証要求を発行する（ステップS8311）。受信ノード8104は、この映像はホームゲートウェイ8103から配信されていると解釈しているため、この認証要求はホームゲートウェイ8103に対して行われる。

【0218】ホームゲートウェイ8103は、第4の実施形態と同様に、内部の変換テーブル8211を参照して、これをホームゲートウェイ8102にフォワードする。これは、ホームゲートウェイ8103は、映像の配信元がホームゲートウェイ8102であると解釈しているからである。このフォワードは、認証要求8311の中身を変えない形で、インターネットパケットで行われる（ステップS8312）。同様に、ホームゲートウェイ8102は、これを受信ノード8101にフォワードする（ステップS8313）。送信ノード8101は、これをホームゲートウェイ8101から発行された認証要求であると解釈する。

【0219】これと同様の手順を双方向に組み、送信ノード8101と受信ノード8104間で認証手続きが行われる（ステップS8314）。この間、ホームゲートウェイは、この手続きのパケットを中身を変更せずにフォワードする。認証と並行して、鍵情報のやり取りを行い、受信ノード8104は鍵の入手を行い、結局、暗号化されたMPEG2映像の復号化ができるようになる。

【0220】しかして、送信ノード8101が送信するMPEG映像を、コンテンツキーKを使って暗号化し、これが1394バスの同期チェネル#x、ホームゲートウェイ8102、公衆網、ホームゲートウェイ8103、1394バスの同期チェネル#yという経路を辿って、受信ノード8103に到達する（ステップS8315～S8317）。そして、受信ノード8103では、暗号化されたMPEG映像は、暗号鍵Kを使って暗号復号化され、デコードされて、再生表示される。

【0221】このように、家庭網とインターネットが相互接続された環境においても、代理機能を提供するホームゲートウェイを介して、送信ノードと受信ノードが認証手続きや鍵交換手続きを行うことで、実際のMPEG映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。このように、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【0222】なお、第5の実施形態において、公衆網の通信帯域が十分に広くない場合には、両ホームゲートウェイにおいて第4の実施形態の符号化変換（例えば、ホームゲートウェイ8102ではMPEG2/MPEG4変換、ホームゲートウェイ8103ではMPEG4/MPEG2変換）を行うことによって、若干の圧縮損はあるものの、両家庭網間でコピープロテクションを考慮したデータ転送を行うことが可能になる。

【0223】（第6の実施形態）第1の実施形態においては、中継ノードがIEEE1394バスと無線網との両方に接続され、IEEE1394バス上の送信ノードと無線網上の無線ノードとの間で暗号化された映像データのやり取りをする場合の、認証・鍵交換方式を説明した。第1の実施形態では、認証フォーマットの交換等に代表される実際の認証・鍵交換は、送信ノードと無線ノード間で直接行ない、中継ノードは、これらのデータを透過的に中継する形で、これを実現してきた。

【0224】これに対し、第6の実施形態では、第2の実施形態のように、認証・鍵交換の単位を送信ノードと中継ノード間、および中継ノードと無線ノード間でそれぞれ行なう。ただし、第2の実施形態と異なり、中継ノ

ードにてコンテンツデータの暗号の復号化、および再暗号化を行なう必要が無いような方法の説明を行なう。すなわち、第２の実施形態では、到着したデータについて、中継ノードにてＩＥＥＥ１３９４区間の暗号の復号化を行い、無線区間の暗号化を再度行なうといった手順を使っていたが、これに対し、第６の実施形態では、ＩＥＥＥ１３９４バス側から到着した暗号化データをそのまま無線網上に転送できるような方法である。

【０２２５】図７７に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第２の実施形態と同様である。

【０２２６】図７８に、送信ノード９１０１の内部構造の一例を示す。これも第２の実施形態と基本的には同様である。認証フォーマットＡｃｅｒｔが、ノードに一つ用意されている。

【０２２７】図７９に、中継ノード９１０２の内部構造の一例を示す。認証フォーマットＢｃｅｒｔ、Ｃｃｅｒｔが、ネットワークインタフェース毎に一つ（ＩＥＥＥ１３９４側にＢｃｅｒｔ、無線網側にＣｃｅｒｔ）用意されている。ＩＥＥＥ１３９４側のＩＳＯ信号送受信部９２０３と無線ＩＳＯ信号送受信部９２０６間で、（復号化／再暗号化のプロセスを経ずに）直接暗号化されたストリーム信号がやり取りされる点を除いて、第２の実施形態と同様である。

【０２２８】図８０に、無線ノード９１０３の内部構造の一例を示す。これも第２の実施形態と基本的には同様である。認証フォーマットＤｃｅｒｔが、ノードに一つ用意されている。

【０２２９】これまでの実施形態と同様に、中継ノードでは、ＩＥＥＥ１３９４側には無線網上のサービスの、無線網側にはＩＥＥＥ１３９４上のサービスのそれぞれ代理サービス機能があるものとする。なお、ここでの詳細な説明は省略する。

【０２３０】次に、本実施形態の全体のシーケンス例を図８１に示す。これまでの実施形態と同様に、例えば中継ノードが、送信ノードが提供しているサービス（映像送信サブユニット）を代理で無線網側に広告しており、無線ノード（の映像デコードサブユニット）が、中継ノードの代理機能に対してサービス（ＭＰＥＧ映像転送要求）を要求、中継ノードが実際のサービスを提供している送信ノードの映像送信サブユニットに対して、実際の映像転送要求を行う。実際の映像データは、暗号化された形でＩＥＥＥ１３９４上は同期チャネル＃ｘ上を、無線網上は無線同期チャネル＃ｙ上を転送されるものとする。なお、詳細はこれまでの実施形態と同様であるので、ここでの詳細な説明は省略する。

【０２３１】また、送信ノード９１０１の動作手順例を図８２に、中継ノード９１０２の動作手順例を図８３／図８４に、無線ノード９１０３の動作手順例を図８５／図８６に、それぞれ示す。

【０２３２】本実施形態では、ＩＥＥＥ１３９４上の著作権保護方式である「５Ｃ Ｄｉｇｉｔａｌ ＴｒａｎｓｍｉｓｓｉｏｎＣｏｎｔｅｎｔ ＰｒｏｔｏｃｔｉｏｎＳｐｅｃｉｆｉｃａｔｉｏｎ」の認証・鍵交換方式に基本的に準ずる手順を踏むものとする。なお、本実施形態では、認証・鍵交換方式をノード単位で行う場合について説明する（サブユニット単位で行う場合については、第７の実施形態で説明する）。

【０２３３】さて、送信ノード９１０１は、ＩＥＥＥ１３９４の同期チャネル＃ｘ上に、コンテンツ鍵Ｋで暗号化されたＭＰＥＧ映像を転送する（ステップＳ８５０１，Ｓ８６０１，Ｓ８７０１）。これを受信した中継ノード９１０２は、このまま（受信したＭＰＥＧ映像を、コンテンツ鍵Ｋで暗号化されたまま）無線網側の無線同期チャネル＃ｙに対して転送する（ステップＳ８５０９，Ｓ８７０１）。

【０２３４】同期チャネル＃ｙを通して受信したデータが暗号化されていると認識した中継ノード９１０２は、到着したデータのＣＩＰヘッダの送信ノードＩＤフィールド（ＳＩＤフィールド）を参照する等して、送信ノード９１０１と認証・鍵交換すべきであると認識する（ステップＳ８８０１）。中継ノード９１０２の認証フォーマットＢｃｅｒｔを含んだ認証要求パケットを送信ノード９１０１に対して転送する（ステップＳ８５０２，Ｓ８７０２）。

【０２３５】これを受信した送信ノード９１０１は、送信ノードの認証フォーマットＡｃｅｒｔを含んだ認証要求パケットを中継ノード９１０２に対して送信する（ステップＳ８５０３，Ｓ８６０２，Ｓ８６０３，Ｓ８７０３）。

【０２３６】次に、認証・鍵交換手続きを行って、送信ノード９１０１と中継ノード９１０２の両者で、認証鍵Ｋａｕｔｈ１を秘密裏に共有する（ステップＳ８５０４，Ｓ８５０５，Ｓ８６０４，Ｓ８７０４）。

【０２３７】ＩＥＥＥ１３９４著作権保護方式では、コンテンツ鍵Ｋは、交換鍵Ｋｘ、シードＮｃ、暗号制御情報ＥＭＩの３つの変数の関数Ｊにて計算される。すなわち、Ｋ＝Ｊ（Ｋｘ，Ｎｃ、ＥＭＩ）である。ここでＥＭＩは転送される暗号化データには必ず付与される値である。よって、送信ノード９１０１は、受信側（中継ノード、本実施形態の場合は無線ノードも）に対して、交換鍵ＫｘとシードＮｃの値を通知する必要がある。

【０２３８】そこで、送信ノード９１０１は、中継ノード９１０２との間で共有した認証鍵Ｋａｕｔｈ１を使って、既知の関数ｆを使って、ｆ（Ｋｘ，Ｋａｕｔｈ）の形で中継ノード９１０２に送信する（ステップＳ８５０６，Ｓ８６０５，Ｓ８７０８，Ｓ８７０９）。中継ノード９１０２は、この値から、Ｋｘの値を算出することができる。同様に、シードＮｃの値も、送信ノード９１０１から中継ノード９１０２に転送される（ステップＳ８

507，S8606，S8710）。ここで、中継ノード9102は、暗号を復号するコンテンツ鍵Kを生成するのに必要なKx，Ncの値をこの時点で認識したことになる。

【0239】さて、同様の手続きが中継ノード9102と無線ノード9103の間でも行われる（ステップS8510～S8513，S8705～S8707，S8802～S8804）。この手続きは、送信ノード9101と中継ノード9102との間の認証・鍵交換手続きと同様であるので、ここでの詳細な説明は省略する。ここで、無線網の無線同期チャネル#y上を転送される暗号化されたデータにも、送信元ノードである中継ノード9102を識別できるようなアドレス情報等が付与されていてもよい。

【0240】さて、中継ノード9102と無線ノード9101とで認証鍵Kauth2が共有できたものとする。本実施形態では、中継ノード9102は、暗号化されたMPEG映像を暗号の復号化をすることなく、そのまま無線網（の無線同期チャネル#y）にフォワード処理を行ってしまうため、中継ノード9102は無線ノード9103に対して、IEEE1394区間と同じ交換鍵KxとシードNcの値を通知する必要がある（逆に通知できれば、無線ノード9103は暗号の復号化が可能である。ただし、IEEE1394区間と無線網区間は、同じコンテンツ保護ポリシーで運営されているものとする）。そこで、中継ノード9102は、S8506、S8507で受信したデータより算出したKx，Ncのそれぞれの値を、同様に無線ノード9103に対して送信する（ステップS8514，S8515，S8709，S8711，S8805～S8807）。具体的には、Kxの値は認証鍵Kauth2の値を使ってf（Kx，Kauth2）を計算して、無線ノード9103に送出し、Ncの値はそのまま転送する。

【0241】無線ノード9103では、このようにして、中継ノードと同じ手順を使ってKx、Ncの値を認識できるため、同様の関数Jを使ってコンテンツ鍵Kの値を算出することができる（ステップS8516）。

【0242】よって、送信ノード9101から送られてくる、コンテンツ鍵Kで暗号化されたMPEG映像は、中継ノード9102で暗号の復号化がなされず、そのままフォワードして無線ノード9103まで転送されてきた場合（ステップS8508，S8517，S8607，S8712，S8809）でも、先にS8516で計算したコンテンツ鍵Kの値を使って、暗号の復号化ができる（ステップS8518，S8810）。その後、MPEG映像のデコード、ディスプレイ表示等が行われる。

【0243】なお、本実施形態では、無線網上では無線同期チャネルが定義されており、暗号化されたMPEG映像はこの無線同期チャネル上を転送されてくるとして説明を行ってきたが、第2の実施形態のように、無線網上でのQOSデータ転送がイーサネットと同様の無線フレームを転送する場合にも、同様の方法（Kx，Ncの値を中継ノードから無線ノードにフォワードする）が適用可能である。

【0244】逆に言うと、本実施形態のような方法により、中継ノード9102では暗号の復号化および再暗号化が不要になり、高速なパケット転送も可能になることから、低コストな中継ノードの構築が可能となる。

【0245】なお、この場合、IEEE1394側に送信ノード9102とは別のノード（別ノード）が存在しており、この別ノードから中継ノード9102を経て、無線ノード9103に別のコンテンツ鍵で暗号化されたデータ（厳密には同じEMIを持ったデータ）を送信することはできない。コンテンツ鍵は、基本的にデータの送信ノード9101が決定する仕組みとなっていることから、別ノードが別のコンテンツ鍵を選択する可能性は十分にある。しかし、中継ノード9102と無線ノード9103との間で、既にコンテンツ鍵Kが一意に定義されている。すなわち、中継ノード9102と無線ノード9103との間では、同じEMI値については、1つのコンテンツ鍵しか共有できない。よって、両ノード間では、高々1つのコンテンツ鍵しか使うことができないため、別ノードからの（別のコンテンツ鍵で暗号化された）データを受信しても、これを中継ノード9102から無線ノード9103に転送する際に、別のコンテンツ鍵を生成できないため、これを復号化できないことになる。

【0246】よって、中継ノード9102は、既に暗号化データを送信しているノード（本実施形態の場合、無線ノード9103）に対して、別のコンテンツ鍵を使う必要のある暗号化データの送信要求があった場合（例えば、IEEE1394の別ノードの代理サービスに対するサービス要求があった場合等）は、これを拒否することにより、未然に上記矛盾を回避することが可能となる。また、中継ノード9102は、既に無線ノード9103に対して暗号化データの送信を行っている場合には、該無線ノード9103に対しては、他のサービス（サブユニット）は見せない（代理サービス提供自体を中断する、あるいは暗号化ストリーム転送を伴う代理サービスの提供を中断する、等）、というやり方でも、同様の効果が考えられる。

【0247】（第7の実施形態）第6の実施形態では、認証・鍵交換の単位を送信ノードと中継ノードとの間、および中継ノードと無線ノードとの間でそれぞれ行ない、中継ノードにて暗号の復号化、および再暗号化を行なう必要が無いような方法であった。

【0248】これに対し、第7の実施形態では、中継ノードにて暗号の復号化、および再暗号化を行なう必要が無いのは同様であるが、無線網側での認証・鍵交換の単

位が、第2の実施形態と同じくサブユニット単位にでき、同じノード間でも複数のコンテンツ鍵を持つことができるような場合である。本実施形態によれば、ＩＥＥＥ１３９４上の複数送信ノードからの暗号化データの同時受信が可能となる。

【０２４９】図８７に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は、送信ノード（ＰとＱ）が2つある点以外、基本的には第６の実施形態と同様である。

【０２５０】送信ノード９８０１，９８１１の内部構成は、第６の実施形態と同様である。

【０２５１】中継ノード９８０２の内部構成は、ＩＥＥＥ１３９４側では認証・鍵交換の単位がノード間であり、無線網側では認証・鍵交換の単位がサブユニット間である点を除いて、第６の実施形態と同様である。

【０２５２】無線ノード９８０３の内部構成は、認証・鍵交換の単位がサブユニット間である点を除いて、第６の実施形態と同様である。

【０２５３】なお、送信ノード９８０１，９８１１、無線ノード９８０２の動作手順は基本的には第６の実施形態と同様である。また、１つの送信ノードに対して中継を行う場合の中継ノード９８０３の動作手順も基本的には第６の実施形態と同様である。

【０２５４】これまでの実施形態と同様に、中継ノードでは、ＩＥＥＥ１３９４側には無線網上のサービスの、無線網側にはＩＥＥＥ１３９４上のサービスのそれぞれ代理サービス機能があるものとする。なお、ここでの詳細な説明は省略する。

【０２５５】次に、複数の送信ノードに対して中継を行う場合の中継ノード９８０２の動作手順例を図８８に、本実施形態の全体のシーケンス例を図８９／図９０に示す。これまでの実施形態と同様に、例えば中継ノードが、送信ノードが提供しているサービス（映像送信サブユニット）を代理で無線網側に広告しており、無線ノード（の映像デコードサブユニット）が、中継ノードの代理機能に対してサービス（ＭＰＥＧ映像転送要求）を要求、中継ノードが実際のサービスを提供している送信ノードの映像送信サブユニットに対して、実際の映像転送要求を行う。実際の映像データは、暗号化された形でＩＥＥＥ１３９４上は同期チャネル＃ｘ上を、無線網上は無線同期チャネル＃ｙ上を転送されるものとする。詳細はこれまでの実施形態と同様であるので、ここでの詳細な説明は省略する。

【０２５６】本実施形態でも、ＩＥＥＥ１３９４上の著作権保護方式である「５Ｃ Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ ＰｒｏｔｏｃｔｉｏｎＳｐｅｃｉｆｉｃａｔｉｏｎ」の認証・鍵交換方式に基本的に準ずる手順を踏むものとする。

【０２５７】さて、送信ノードＰ（９８０１）は、ＩＥＥＥ１３９４の同期チャネル＃ｘ上に、コンテンツ鍵Ｋ１で暗号化されたＭＰＥＧ映像を転送する（ステップＳ９２０１，Ｓ９３０１）。第６の実施形態と同様に、コンテンツ鍵Ｋ１は、Ｋ１＝Ｊ（Ｋｘｐ，Ｎｃｐ，ＥＭＩ）にて計算されるものとする。これを受信した中継ノード９８０２は、このまま（受信したＭＰＥＧ映像を、コンテンツ鍵Ｋ１で暗号化されたまま）無線網側の無線同期チャネル＃ｙに対して転送する（ステップＳ９２０９，Ｓ９３０１）。

【０２５８】中継ノード９８０２が送信ノードＰに対して認証要求をし、鍵交換などを行って、交換鍵ＫｘｐとシードＮｃｐを獲得する手順（ステップＳ９２０２～Ｓ９２０７，Ｓ９３０２）は、第６の実施形態と同様であるので、ここでの詳細な説明は省略する。この時点で、中継ノード９８０２は暗号を復号するために必要なＫｘｐ，Ｎｃｐの値を認識したことになる。

【０２５９】さて、同様の認証・鍵交換手続きが中継ノード９８０２と無線ノード９８０３の間でも行われる（ステップＳ９２１０～Ｓ９２１７，Ｓ９３０３）。この手続きは第２の実施形態の送信ノードと中継ノード間の認証・鍵交換手続きと同様であるので、ここでの詳細な説明は省略する。ただし、認証先問い合わせや認証先応答、あるいは認証要求にサブユニットのＩＤの他、チャネル番号、あるいは暗号化データの送受信を行うことになるプラグの識別子を搭載して、これを行ってもよい。中継ノード９８０２、あるいは無線ノード９８０３が、「どの暗号化データについての認証・鍵交換手続きか」ということが識別できるようになり、後述するように、異なる鍵の暗号化データについては、同一のノード間の認証・鍵交換であったとしても、異なる鍵を通知することが可能になる。

【０２６０】なお、この際、認証要求にチャネル番号を含める場合は、ステップＳ９２１０の認証先問い合わせとステップＳ９２１１の認証先応答は不要となる。

【０２６１】さて、中継ノード９８０２と無線ノード９８０３で認証鍵Ｋａｕｔｈ１が共有できたものとする。本実施形態でも、中継ノード９８０２は、暗号化されたＭＰＥＧ映像を暗号の復号化をすることなく、そのまま無線網（の無線同期チャネル＃ｙ）にフォワード処理を行ってしまうため、中継ノード９８０２は無線ノード９８０３に対して、交換鍵ＫｘｐとシードＮｃｐの値を通知する必要がある（逆に通知できれば、無線ノード９８０３は暗号の復号化が可能である）。そこで、中継ノード９８０２は、Ｓ９２０６、Ｓ９２０７で受信したデータより算出したＫｘｐ，Ｎｃｐのそれぞれの値を、同様に無線ノード９８０３に対して送信する（ステップＳ９２１６，Ｓ９２１７）。Ｋｘｐの値は認証鍵Ｋａｕｔｈ１の値を使ってｆ（Ｋｘｐ，Ｋａｕｔｈ１）を計算して、無線ノード９８０３に送出する（ステップＳ９２１６）。

【０２６２】無線ノード９８０３では、このようにし

て、中継ノード９８０２と同じ手順を使ってＫｘｐ、Ｎｃｐの値を認識できるため、同様の関数Ｊを使ってコンテンツ鍵Ｋ１の値を算出することができる（ステップＳ９２１８）。

【０２６３】よって、送信ノードＰから送られてくる、コンテンツ鍵Ｋ１で暗号化されたＭＰＥＧ映像は、中継ノード９８０２で暗号の復号化をせずに、そのままフォワードして無線ノード９８０３まで転送されてきた場合（ステップＳ９２０８，Ｓ９２１９）でも、先にステップＳ９２１８で計算したコンテンツ鍵Ｋ１の値を使って、暗号の復号化ができる（ステップＳ９２２０）。その後、ＭＰＥＧ映像のデコード、ディスプレイ表示等が行われる。

【０２６４】本実施形態のような方法でも、中継ノード９８０２では暗号の復号化、および再暗号化が不要になり、高速なパケット転送も可能になることから、低コストな中継ノードの構築が可能となる。

【０２６５】さて、次に、別の送信ノードＱ（９８１１）が、同時に中継ノード９８０２を介して無線ノード９８０３に対して別のコンテンツ鍵Ｋ２で暗号化されたデータを送信する場合（ステップＳ９２２１，Ｓ９２２９，Ｓ９３０４）を考える。

【０２６６】本実施形態の前半と同様に、送信ノードＱと中継ノード９８０２との間で認証・鍵交換が行われ（ステップＳ９２２２～Ｓ９２２７）、中継ノード９８０２は交換鍵ＫｘｑとシードＮｃｑの値をそれぞれ得ることができる。

【０２６７】本実施形態においては、中継ノード９８０２と無線ノード９８０３との間の認証は、サブユニット間単位であるので、暗号化データの送受が異なるサブユニット間で行われているものとすれば、中継ノード９８０２と無線ノード９８０３との間で複数の認証・鍵交換が可能となる。

【０２６８】すなわち、本実施形態の前半と同様に、中継ノード９８０２と無線ノード９８０３との間で、本実施形態の前半とは異なるサブユニット間で認証・鍵交換を行っていく（ステップＳ９２３０～Ｓ９２３５，Ｓ９３０５）。その上で、中継ノード９８０２は、送信ノードＱと自ノード（中継ノード）９８０２との間の交換鍵ＫｘｑとシードＮｃｑを、無線ノード９８０３にフォワードする（ステップＳ９２３６，Ｓ９２３７，Ｓ９３０５，Ｓ９３０６）。

【０２６９】無線ノード９８０３では、このようにして、Ｋｘｑ、Ｎｃｑの値を認識できるため、同様の関数Ｊを使ってコンテンツ鍵Ｋ２の値を算出することができる（ステップＳ９２３８）。

【０２７０】よって、送信ノードＱから送られてくる、コンテンツ鍵Ｋ２で暗号化されたＭＰＥＧ映像は、中継ノード９８０２で暗号の復号化をせずに、そのままフォワードして無線ノード９８０３まで転送されてきた場合（ステップＳ９２２８，Ｓ９２２９）でも、先にステップＳ９２３８で計算したコンテンツ鍵Ｋ２の値を使って、暗号の復号化ができる（ステップＳ９２４０）。つまり、２つの異なるコンテンツ鍵（本実施形態ではＫ１とＫ２）で暗号化されたＭＰＥＧ映像の同時受信が可能となる。

【０２７１】なお、第６の実施形態と第７の実施形態では、ＩＥＥＥ１３９４と無線網との相互接続を行う場合を例に説明してきたが、インターネット等のその他の網についても適用可能である。

【０２７２】なお、第１～第７の実施形態において例示したデータ転送の方向とは逆の方向にデータ転送する場合（例えば、無線ノードからＩＥＥＥ１３９４上のノードへデータ転送する場合）にも、本発明は適用可能である。

【０２７３】また、第１～第７の実施形態において、無線ノードやＩＥＥＥ１３９４上のノードについては、コンテンツについて送信機能または受信機能の一方に着目して説明したが、無線ノードやＩＥＥＥ１３９４上のノードは、コンテンツについて送信機能と受信機能の両方を備えることも可能である。

【０２７４】また、認証手続きや、鍵交換手続き（コンテンツ鍵共有手続き）は、これまでに例示したものに限定されず、他の種々の方法が用いられる場合にも本発明は適用可能である。

【０２７５】また、以上では、家庭網ネットワークとして実施形態を説明したが、もちろん、本発明は家庭網以外のネットワークにも適用可能である。

【０２７６】なお、以上の各機能は、ソフトウェアとしても実現可能である。

【０２７７】また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【０２７８】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０２７９】

【発明の効果】本発明によれば、同じネットワークでは接続されていない装置間で、保護すべきコンテンツの送受信のためのコンテンツ保護手続きを行うことが可能になる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るネットワークの全体構成の一例を示す図

【図２】送信ノードの内部構造の一例を示す図

【図３】中継ノードの内部構造の一例を示す図

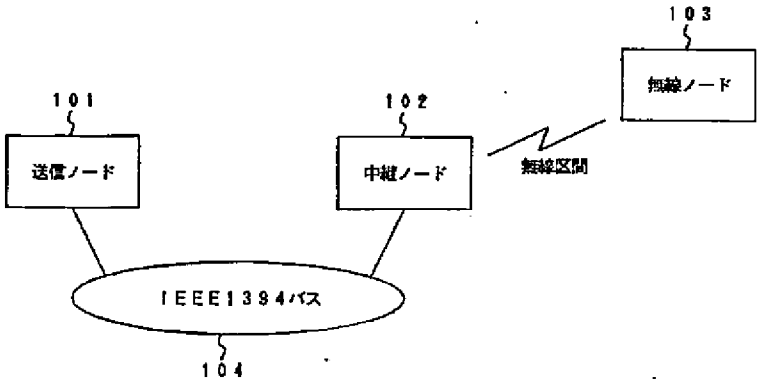
【図４】無線ノードの内部構造の一例を示す図

【図５】全体のシーケンスの一例を示す図
【図６】全体のシーケンスの一例を示す図
【図７】送信ノードの動作手順の一例を示すフローチャート
【図８】送信ノードの動作手順の一例を示すフローチャート
【図９】中継ノードの動作手順の一例を示すフローチャート
【図１０】中継ノードの動作手順の一例を示すフローチャート
【図１１】中継ノードの動作手順の一例を示すフローチャート
【図１２】無線ノードの動作手順の一例を示すフローチャート
【図１３】無線ノードの動作手順の一例を示すフローチャート
【図１４】無線ノード構成情報パケットの一例を示す図
【図１５】代理テーブルの一例を示す図
【図１６】代理テーブルの一例を示す図
【図１７】送信ノードから見た中継ノードの内部構造を説明するための図
【図１８】無線ノードから見た中継ノードの内部構造を説明するための図
【図１９】無線ノード制御パケットの一例を示す図
【図２０】本発明の第２の実施形態に係るネットワークの全体構成の一例を示す図
【図２１】送信ノードの内部構造の一例を示す図
【図２２】中継ノードの内部構造の一例を示す図
【図２３】無線ノードの内部構造の一例を示す図
【図２４】全体のシーケンスの一例を示す図
【図２５】全体のシーケンスの一例を示す図
【図２６】送信ノードの動作手順の一例を示すフローチャート
【図２７】送信ノードの動作手順の一例を示すフローチャート
【図２８】中継ノードの動作手順の一例を示すフローチャート
【図２９】中継ノードの動作手順の一例を示すフローチャート
【図３０】中継ノードの動作手順の一例を示すフローチャート
【図３１】中継ノードの動作手順の一例を示すフローチャート
【図３２】無線ノードの動作手順の一例を示すフローチャート
【図３３】無線ノードの動作手順の一例を示すフローチャート
【図３４】代理テーブルの一例を示す図
【図３５】代理テーブルの一例を示す図
【図３６】送信ノードから見た中継ノードの内部構造を説明するための図
【図３７】無線ノードから見た中継ノードの内部構造を説明するための図
【図３８】無線フレームのフォーマットの一例を示す図
【図３９】無線制御パケットのフォーマットの一例を示す図
【図４０】本発明の第３の実施形態に係るネットワークの全体構成の一例を示す図
【図４１】送信ノードの内部構造の一例を示す図
【図４２】中継ノードの内部構造の一例を示す図
【図４３】無線ノードの内部構造の一例を示す図
【図４４】全体のシーケンスの一例を示す図
【図４５】全体のシーケンスの一例を示す図
【図４６】送信ノードの動作手順の一例を示すフローチャート
【図４７】送信ノードの動作手順の一例を示すフローチャート
【図４８】中継ノードの動作手順の一例を示すフローチャート
【図４９】中継ノードの動作手順の一例を示すフローチャート
【図５０】中継ノードの動作手順の一例を示すフローチャート
【図５１】無線ノードの動作手順の一例を示すフローチャート
【図５２】無線ノードの動作手順の一例を示すフローチャート
【図５３】代理テーブルの一例を示す図
【図５４】代理テーブルの一例を示す図
【図５５】送信ノードから見た中継ノードの内部構造を説明するための図
【図５６】無線ノードから見た中継ノードの内部構造を説明するための図
【図５７】無線ノードに送られてきた制御画面の一例を示す図
【図５８】本発明の第４の実施形態に係るネットワークの全体構成の一例を示す図
【図５９】送信ノードの内部構造の一例を示す図
【図６０】ホームゲートウェイの内部構造の一例を示す図
【図６１】受信ノードの内部構造の一例を示す図
【図６２】全体のシーケンスの一例を示す図
【図６３】全体のシーケンスの一例を示す図
【図６４】送信ノードの動作手順の一例を示すフローチャート
【図６５】送信ノードの動作手順の一例を示すフローチャート
【図６６】ホームゲートウェイの動作手順の一例を示すフローチャート
【図６７】ホームゲートウェイの動作手順の一例を示す

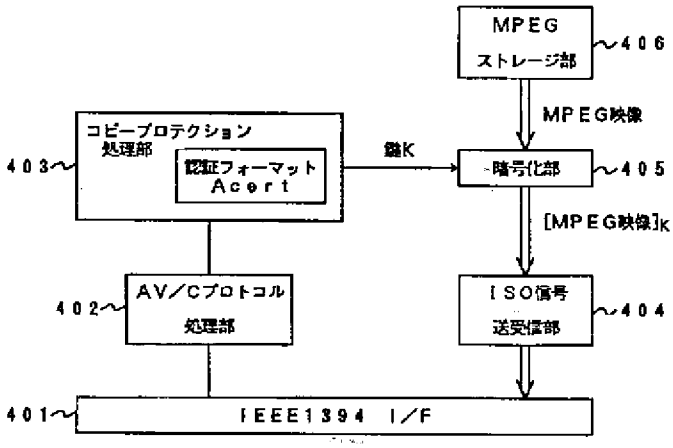
フローチャート
【図68】ホームゲートウェイの動作手順の一例を示すフローチャート
【図69】ホームゲートウェイの動作手順の一例を示すフローチャート
【図70】受信ノードの動作手順の一例を示すフローチャート
【図71】受信ノードの動作手順の一例を示すフローチャート
【図72】送信ノードのパネルとホームゲートウェイの送信ノード制御用ホームページの一例を示す図
【図73】本発明の第5の実施形態に係るネットワークの全体構成の一例を示す図
【図74】ホームゲートウェイの内部構造の一例を示す図
【図75】全体のシーケンスの一例を示す図
【図76】制御画面の一例を示す図
【図77】本発明の第6の実施形態に係るネットワークの全体構成の一例を示す図
【図78】送信ノードの内部構造の一例を示す図
【図79】中継ノードの内部構造の一例を示す図
【図80】無線ノードの内部構造の一例を示す図
【図81】全体のシーケンスの一例を示す図
【図82】送信ノードの動作手順の一例を示すフローチャート
【図83】中継ノードの動作手順の一例を示すフローチャート
【図84】中継ノードの動作手順の一例を示すフローチャート
【図85】無線ノードの動作手順の一例を示すフローチャート
【図86】無線ノードの動作手順の一例を示すフローチャート
【図87】本発明の第7の実施形態に係るネットワークの全体構成の一例を示す図
【図88】中継ノードの動作手順の一例を示すフローチャート
【図89】全体のシーケンスの一例を示す図
【図90】全体のシーケンスの一例を示す図
【符号の説明】
101，2101，4101，6101，8101，9101，9801，9811…送信ノード
102，2102，4102，9102，9802…中継ノード
103，2103，4103，6104，9103，9803…無線ノード
6102，8102，8103…ホームゲートウェイ
6103，8104…受信ノード
104，2104，4104，8105，8107，9104，9804…IEEE1394バス
6105，8106…公衆網
201，2201，4201，6201，8201，9101…IEEE1394インタフェース
202，2202，4202，9202…無線インタフェース
203，2207，4203，6207，8203，9207…AV／Cプロトコル処理部
204，2203，4204，6203，8204，9203…ISO信号送受信部
205，2206，4205，9206…無線ISO信号送受信部
206，2209，4206，6209，9209…1394バス構成認識部
207，2210，4207，8207，9210…代理サブユニット構成部
208，2214，4208，6215，9214…代理テーブル
209，2211，4209，9211…無線区間構成認識部
210，4210，8209…コピープロテクション制御／フォワード部
2208，6208…IEEE1394コピープロテクション処理部
2212，9212…無線区間コピープロテクション部
8211…変換テーブル
211，2213，4211，9213…無線ノード制御パケット送受信部
2204，6204…暗号復号化部
2205，6205…暗号化部
4212…HAVi処理部
4213…IEEE1212レジスタ
6206，8205…AV信号送受信部
6202，8202…インターネットインタフェース
6210，8208…代理ホームページ作成部
6211，8210…ホームページ作成・蓄積部
6212…インターネット側プロテクション処理部
6213…制御パケット送受信部
6214…MPEG2／MPEG4変換部
6206…制御パケット処理信部
301，2301，4301，9301…無線インタフェース
302，2302，4302，9302…無線ノード制御パケット送受信部
303，2303，4303，6303，9303…コピープロテクション処理部
304，2304，4304，9304…無線ISO信号送受信部
305，2305，4305，6305，9305…暗号復号化部
306，2306，4306，6306，9306…M

PEGデコード部
307，2307，4307，6307，9307…ディスプレイ部
6301…インターネットインタフェース
6302…制御パケット送受信部
6304…AV信号送受信部
401，2401，4401，6401，9401…IEEE1394インタフェース
402，2402，4402，6402，9402…AV／Cプロトコル処理部
403，2403，4403，6403，9403…コピープロテクション処理部
404，2404，4404，6404，9404…ISO信号送受信部
405，2405，4405，6405，9405…暗号化部
406，2406，4406，6406，9406…MPEGストレージ部
4407…IEEE1212レジスタ

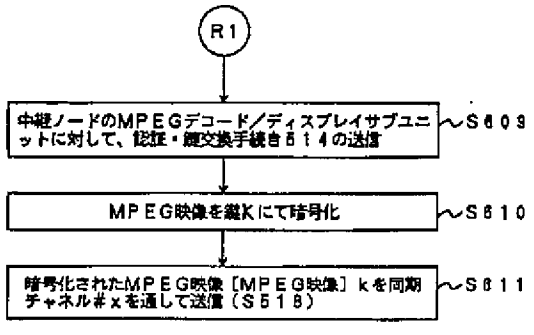
【図1】



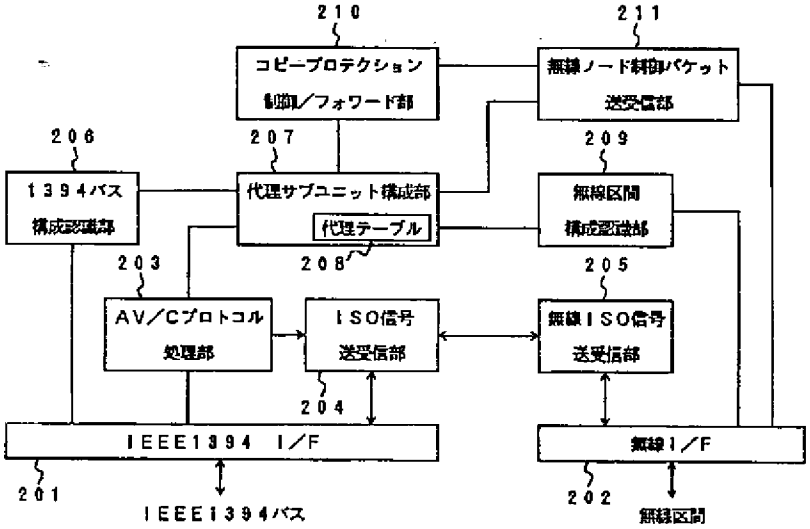
【図2】



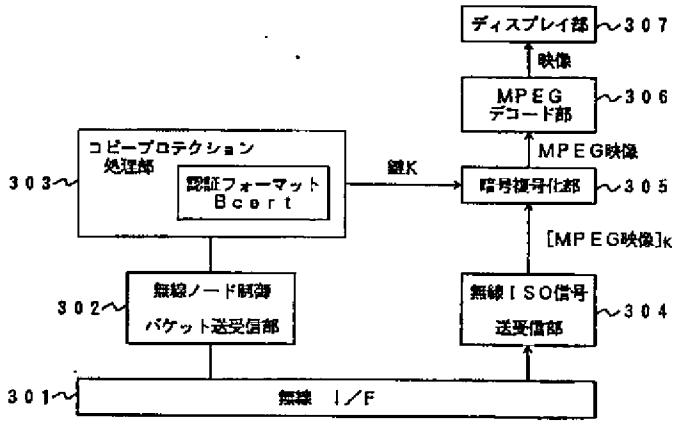
【図8】



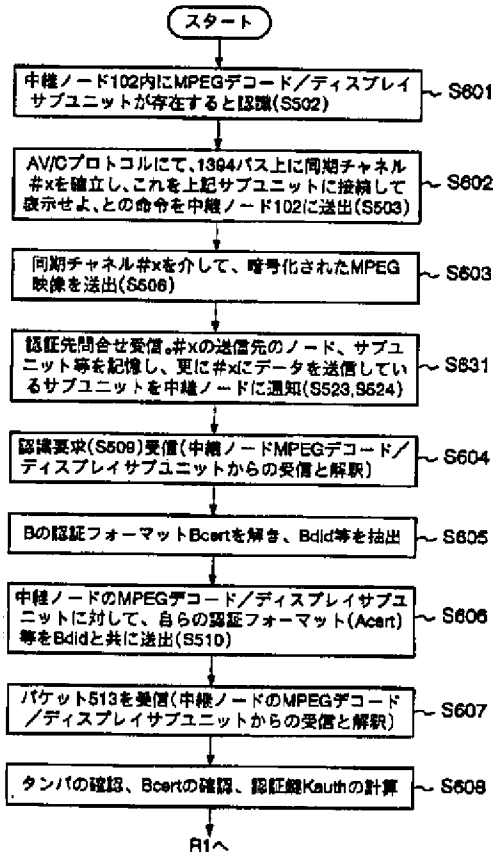
【図3】


210
211
コピープロテクション
制御／フォワード部
無線ノード制御パケット
送受信部
206
207
209
1394バス
構成認識部
代理サブユニット構成部
代理テーブル
無線区間
構成認識部
208
203
205
AV／Cプロトコル
処理部
ISO信号
送受信部
無線ISO信号
送受信部
204
IEEE1394 I／F
無線I／F
201
202
IEEE1394バス
無線区間

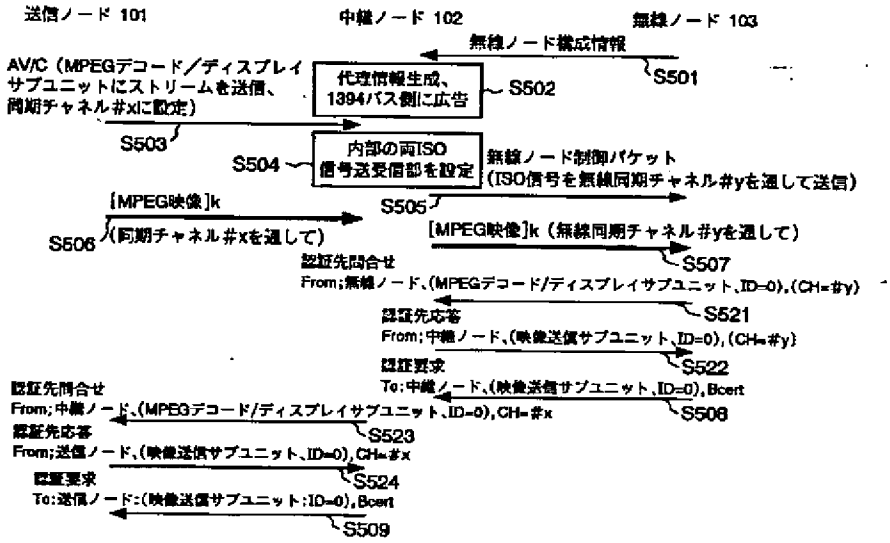
【図4】


ディスプレイ部
307
映像
MPEG
デコード部
306
コピープロテクション
処理部
認証フォーマット
Bcert
303
鍵K
MPEG映像
暗号復号化部
305
[MPEG映像]k
無線ノード制御
パケット送受信部
302
無線ISO信号
送受信部
304
無線 I／F
301

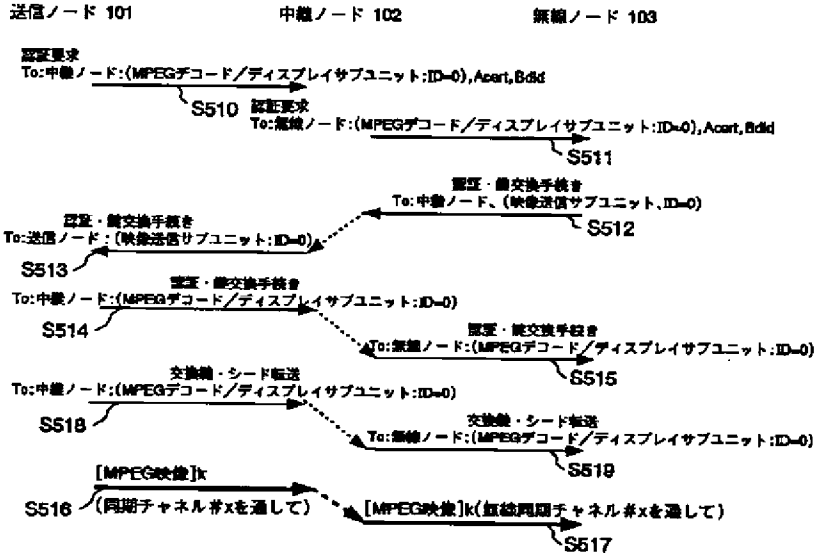
【図7】


スタート
中継ノード102内にMPEGデコード／ディスプレイサブユニットが存在すると認識(S502)
S601
AV/Cプロトコルにて、1394バス上に同期チャネル#xを確立し、これを上記サブユニットに接続して表示せよ、との命令を中継ノード102に送出(S503)
S602
同期チャネル#xを介して、暗号化されたMPEG映像を送出(S506)
S603
認証先問合せ受信。#xの送信先のノード、サブユニット等を記憶し、更に#xにデータを送信しているサブユニットを中継ノードに通知(S523,S524)
S831
認識要求(S509)受信(中継ノードMPEGデコード／ディスプレイサブユニットからの受信と解釈)
S604
Bの認証フォーマットBcertを解き、Bdid等を抽出
S605
中継ノードのMPEGデコード／ディスプレイサブユニットに対して、自らの認証フォーマット(Acert)等をBdidと共に送出(S510)
S606
パケット513を受信(中継ノードのMPEGデコード／ディスプレイサブユニットからの受信と解釈)
S607
タンパの確認、Bcertの確認、認証鍵Kauthの計算
S608
R1へ

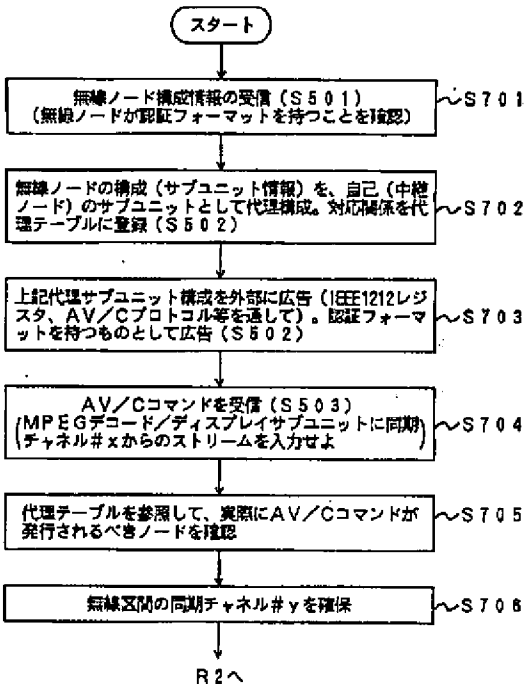
【図5】


送信ノード 101
中継ノード 102
無線ノード 103
無線ノード構成情報
S501
AV/C（MPEGデコード／ディスプレイサブユニットにストリームを送信、同期チャネル#xに設定）
代理情報生成、1394バス側に広告
S502
S503
S504
内部の両ISO信号送受信部を設定
無線ノード制御パケット（ISO信号を無線同期チャネル#yを通して送信）
S505
[MPEG映像]k
S506
（同期チャネル#xを通して）
[MPEG映像]k（無線同期チャネル#yを通して）
S507
認証先問合せ
From;無線ノード、(MPEGデコード/ディスプレイサブユニット、ID=0)、(CH=#y)
S521
認証先応答
From;中継ノード、(映像送信サブユニット、ID=0)、(CH=#y)
S522
認証要求
To:中継ノード、(映像送信サブユニット、ID=0)、Bcert
S508
認証先問合せ
From;中継ノード、(MPEGデコード/ディスプレイサブユニット、ID=0)、CH=#x
S523
認証先応答
From;送信ノード、(映像送信サブユニット、ID=0)、CH=#x
S524
認証要求
To:送信ノード:(映像送信サブユニット:ID=0)、Bcert
S509

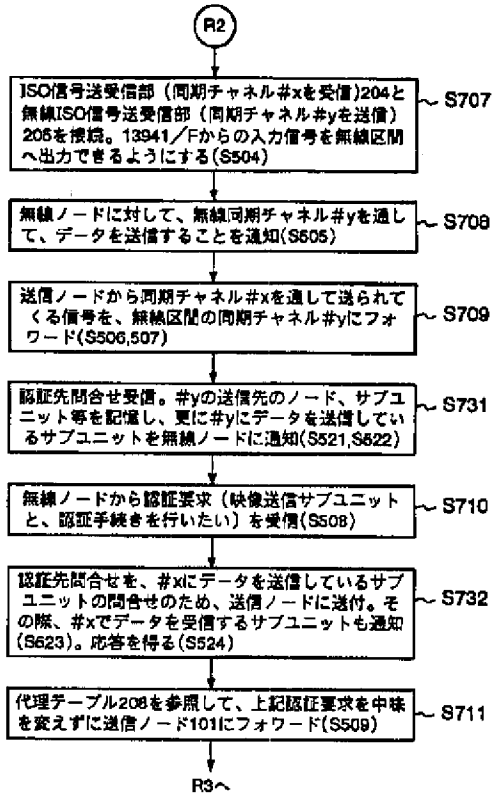
【図6】


送信ノード 101
中継ノード 102
無線ノード 103
認証要求
To:中継ノード:(MPEGデコード／ディスプレイサブユニット:ID=0)、Acert、Bdid
S510
認証要求
To:無線ノード:(MPEGデコード／ディスプレイサブユニット:ID=0)、Acert、Bdid
S511
認証・鍵交換手続き
To:中継ノード、(映像送信サブユニット、ID=0)
S512
認証・鍵交換手続き
To:送信ノード：(映像送信サブユニット:ID=0)
S513
認証・鍵交換手続き
To:中継ノード:(MPEGデコード／ディスプレイサブユニット:ID=0)
S514
認証・鍵交換手続き
To:無線ノード:(MPEGデコード／ディスプレイサブユニット:ID=0)
S515
交換鍵・シード転送
To:中継ノード:(MPEGデコード／ディスプレイサブユニット:ID=0)
S518
交換鍵・シード転送
To:無線ノード:(MPEGデコード／ディスプレイサブユニット:ID=0)
S519
[MPEG映像]k
S516
（同期チャネル#xを通して）
[MPEG映像]k(無線同期チャネル#xを通して)
S517

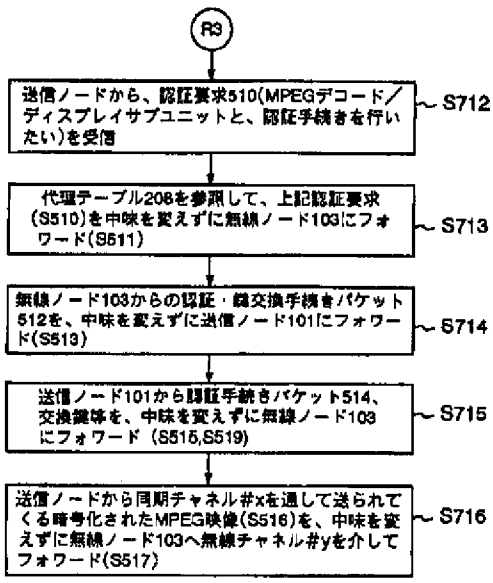
【図９】



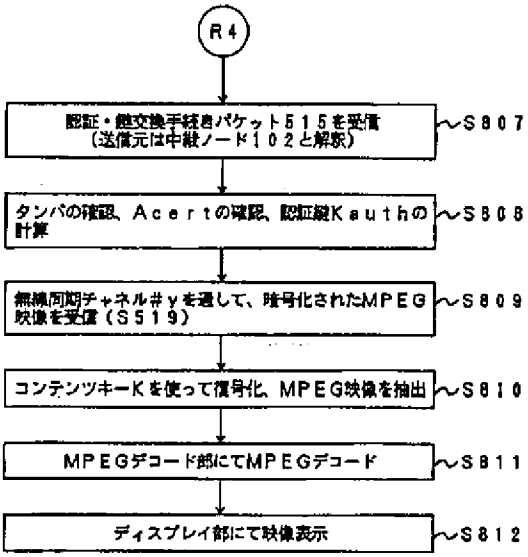
【図１０】



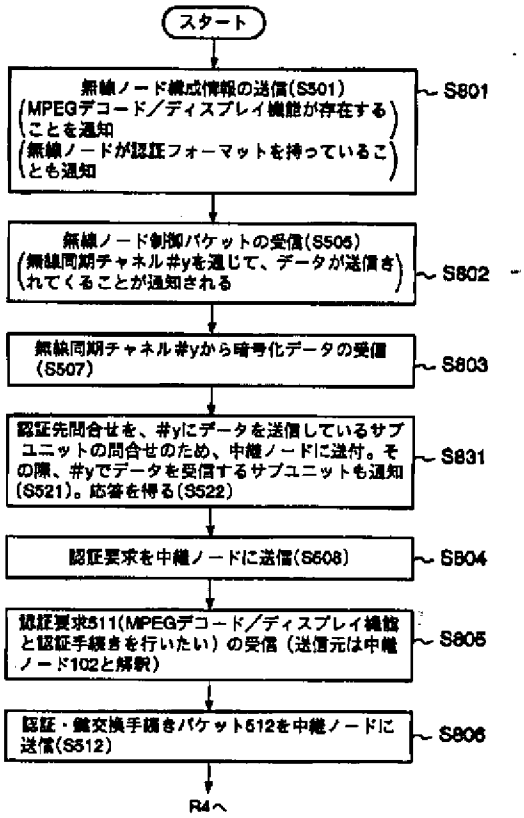
【図１１】



【図１３】



【図１２】



【図１４】

宛先ノード＝中継ノード
送信元ノード＝無線ノード
構成１＝ＭＰＥＧデコード／ディスプレイ機能
構成２＝ …
⋮
構成１の属性１＝認証フォーマット （認証規則＝…）
構成１の属性２＝ＭＰＥＧの上限ビットレート６Ｍｂｐｓ
⋮

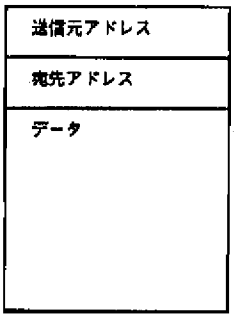
【図１５】

無線区間側の実体	中継ノードが１３９４側に代理サービスする形態
無線ノード１０３の ＭＰＥＧデコード／ディスプレイ機能 （サブユニットID=0） （認証フォーマット有）	ＭＰＥＧデコード／ディスプレイサブユニット （サブユニットID=0） （認証フォーマット有）
⋮	⋮

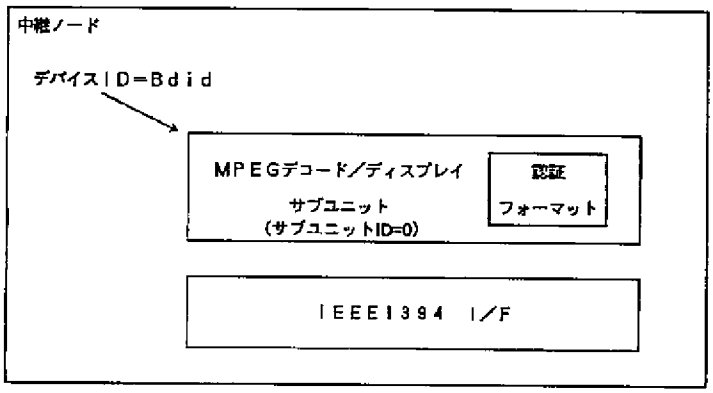
【図16】

1394バス側の実体	中継ノードが無線区間側に代理サービスする形態
送信ノード101の映像送信機能 (映像送信サブユニット) (サブユニットID=0) (認証フォーマット有)	映像送信サブユニット (サブユニットID=0) (認証フォーマット有)
⋮	⋮

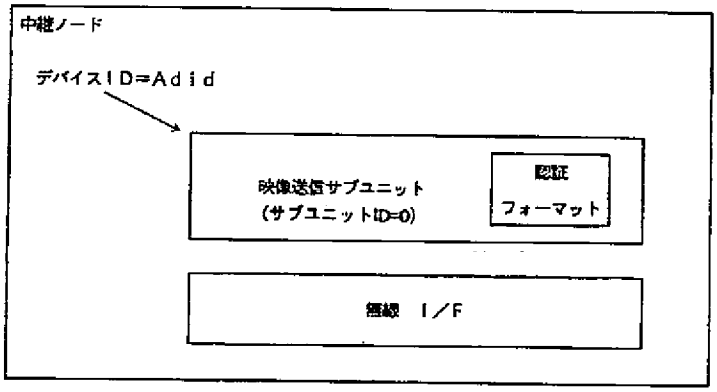
【図38】



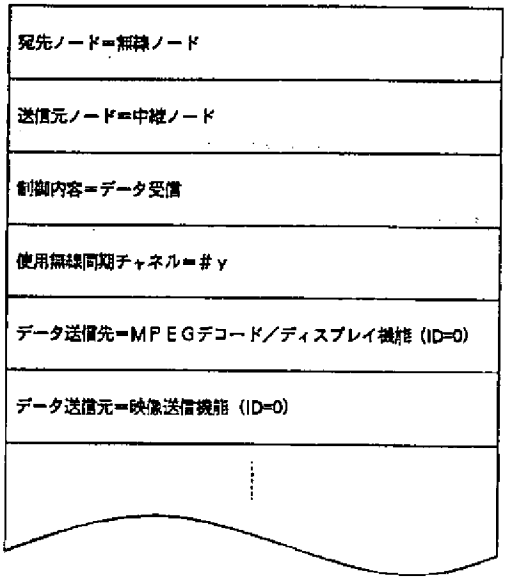
【図17】



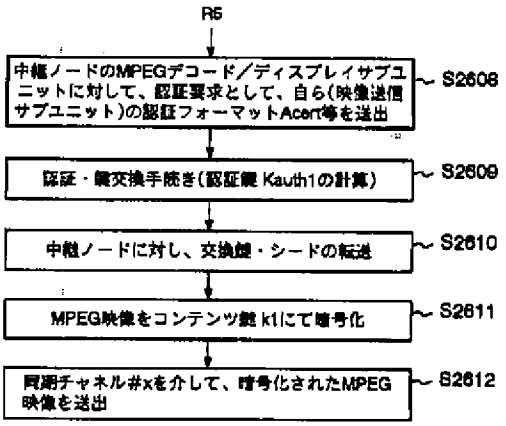
【図18】



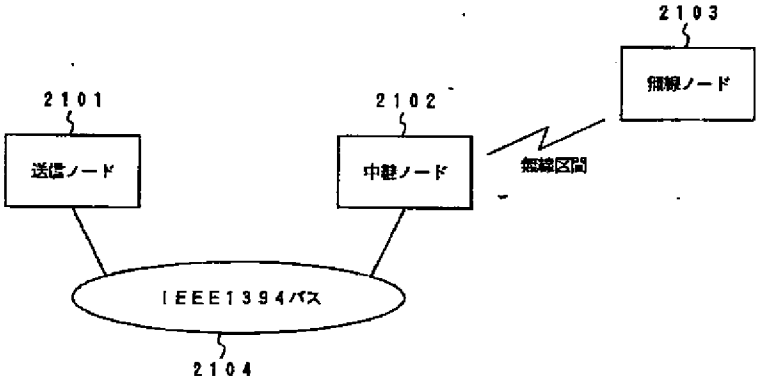
【図19】



【図27】



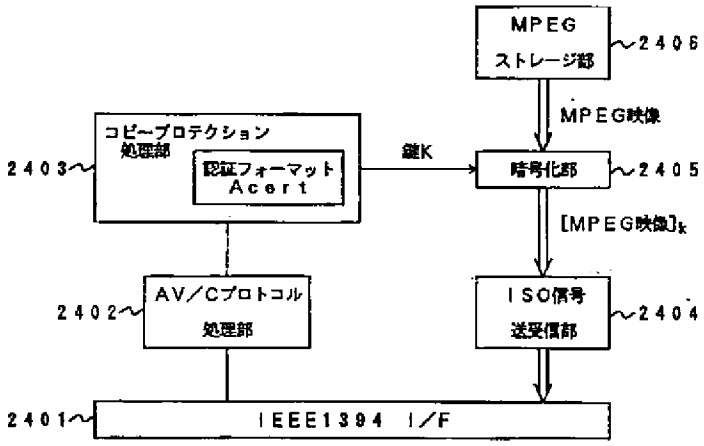
【図20】



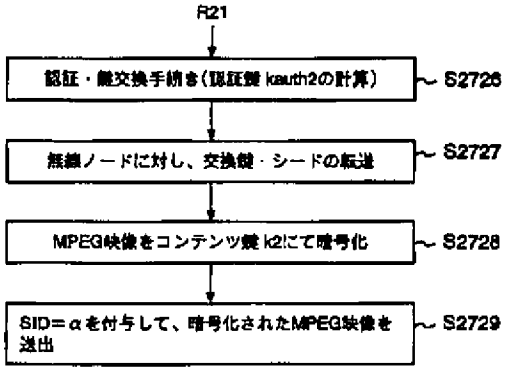
【図39】

宛先ノード＝無線ノード
送信元ノード＝中継ノード
制御内容＝データ受信
使用SID＝α
データ送信先＝ MPEGデコード／ディスプレイ サブユニット（サブユニットID=0）
データ送信元＝ 映像送信サブユニット （サブユニットID=0）

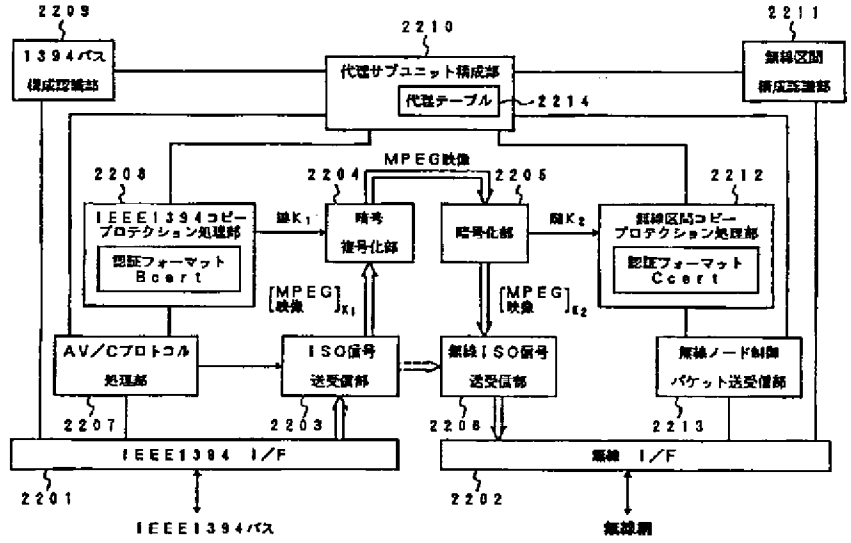
【図21】



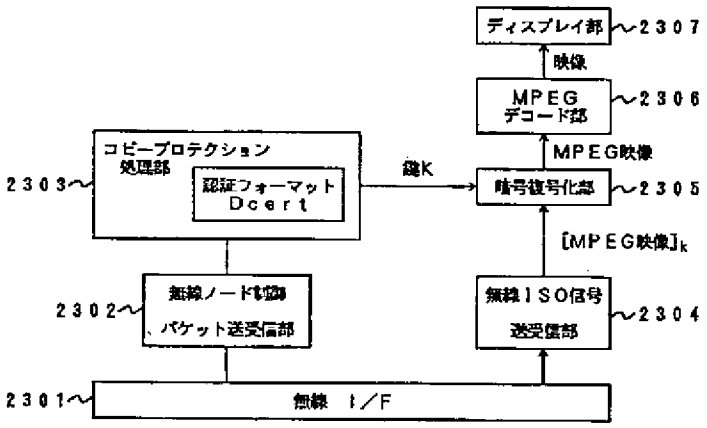
【図31】



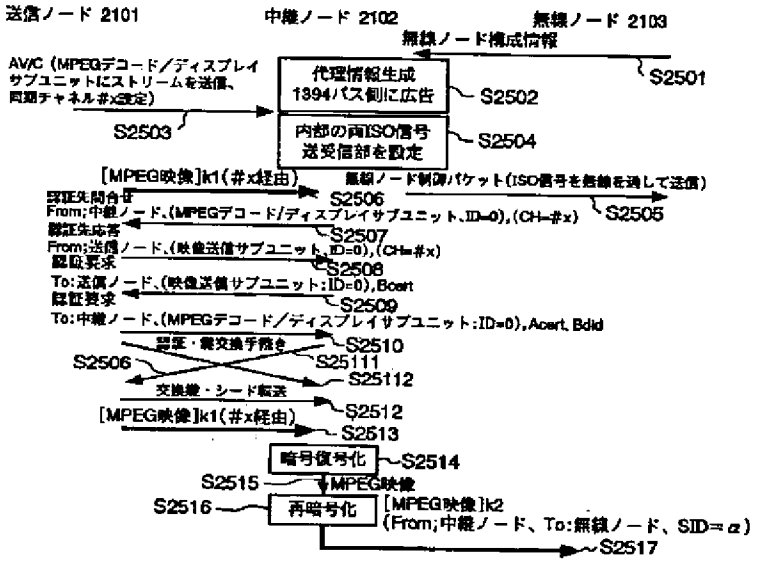
【図22】



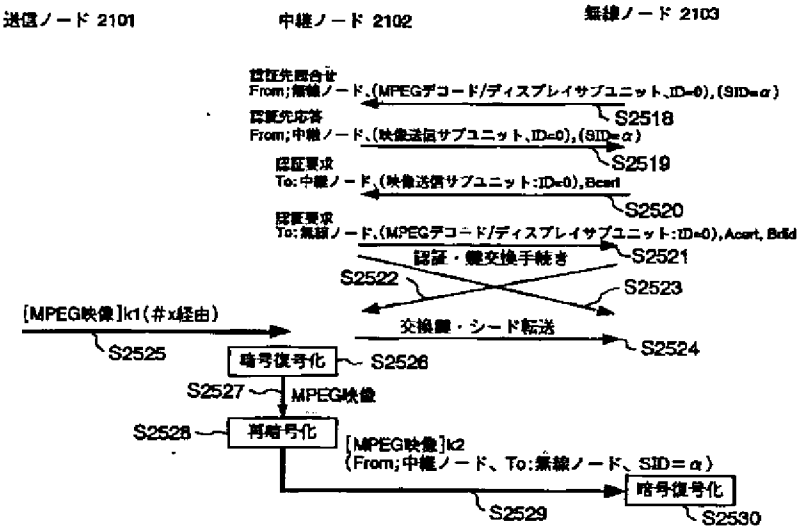
【図23】


ディスプレイ部
2307
映像
MPEG
デコード部
2306
MPEG映像
コピープロテクション
処理部
2303
認証フォーマット
Dcert
鍵K
暗号復号化部
2305
[MPEG映像]k
無線ノード制御
パケット送受信部
2302
無線ISO信号
送受信部
2304
2301
無線 I/F

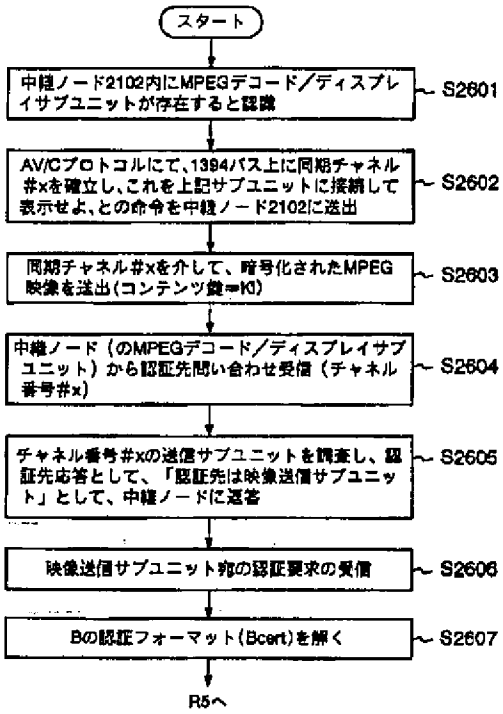
【図24】


送信ノード 2101
中継ノード 2102
無線ノード 2103
無線ノード構成情報
S2501
AV/C (MPEGデコード/ディスプレイ
サブユニットにストリームを送信、
同期チャネル#xに設定)
代理情報生成
1394バス側に広告
S2502
S2503
内部の両ISO信号
送受信部を設定
S2504
[MPEG映像]k1(#x経由)
無線ノード制御パケット(ISO信号を無線を通して送信)
S2506
S2505
認証先問合せ
From:中継ノード,(MPEGデコード/ディスプレイサブユニット,ID=0),(CH=#x)
認証先応答
S2507
From:送信ノード,(映像送信サブユニット,ID=0),(CH=#x)
鍵取要求
S2508
To:送信ノード,(映像送信サブユニット:ID=0),Bcert
鍵証要求
S2509
To:中継ノード,(MPEGデコード/ディスプレイサブユニット:ID=0),Acert, Bdid
認証・鍵交換手続き
S2510
S25111
S2506
S25112
交換鍵・シード転送
S2512
[MPEG映像]k1(#x経由)
S2513
暗号復号化
S2514
S2515
MPEG映像
S2516
再暗号化
[MPEG映像]k2
(From:中継ノード、To:無線ノード、SID=α)
S2517

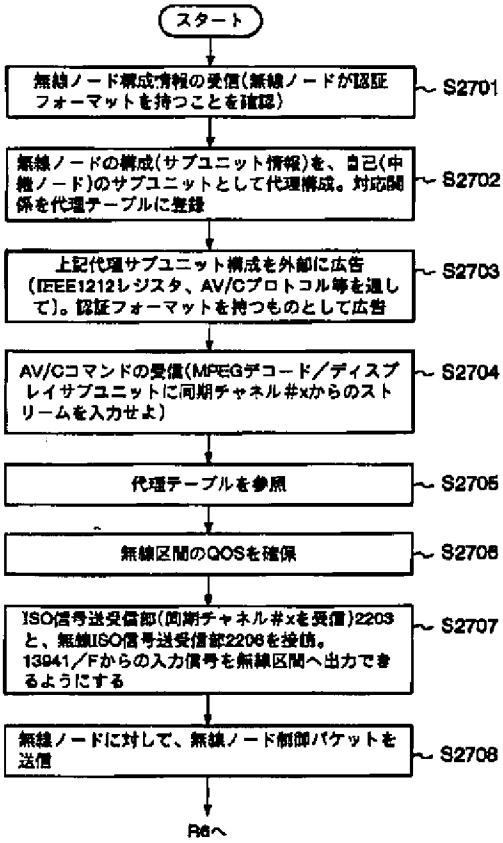
【図25】


送信ノード 2101
中継ノード 2102
無線ノード 2103
認証先問合せ
From;無線ノード,(MPEGデコード/ディスプレイサブユニット,ID=0),(SID=α)
S2518
認証先応答
From;中継ノード,(映像送信サブユニット,ID=0),(SID=α)
S2519
認証要求
To:中継ノード,(映像送信サブユニット:ID=0),Bcert
S2520
認証要求
To:無線ノード,(MPEGデコード/ディスプレイサブユニット:ID=0),Acert, Bdid
認証・鍵交換手続き
S2521
S2522
S2523
[MPEG映像]k1(#x経由)
交換鍵・シード転送
S2524
S2525
暗号復号化
S2526
S2527
MPEG映像
S2528
再暗号化
[MPEG映像]k2
(From;中継ノード、To:無線ノード、SID=α)
暗号復号化
S2529
S2530

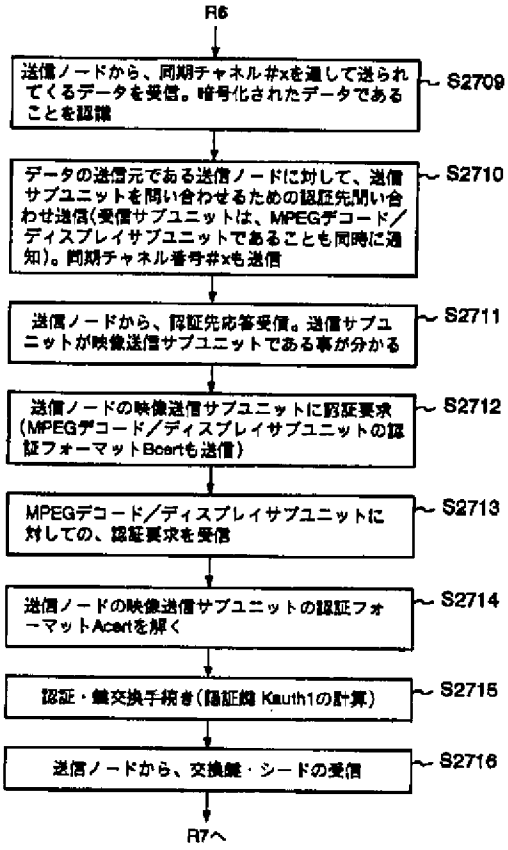
【図26】


スタート
中継ノード2102内にMPEGデコード/ディスプレイサブユニットが存在すると認識
S2601
AV/Cプロトコルにて、1394バス上に同期チャネル#xを確立し、これを上記サブユニットに接続して表示せよ、との命令を中継ノード2102に送出
S2602
同期チャネル#xを介して、暗号化されたMPEG映像を送出(コンテンツ鍵=k1)
S2603
中継ノード(のMPEGデコード/ディスプレイサブユニット)から認証先問い合わせ受信(チャネル番号#x)
S2604
チャネル番号#xの送信サブユニットを調査し、認証先応答として、「認証先は映像送信サブユニット」として、中継ノードに返答
S2605
映像送信サブユニット宛の認証要求の受信
S2606
Bの認証フォーマット(Bcert)を解く
S2607
R5へ

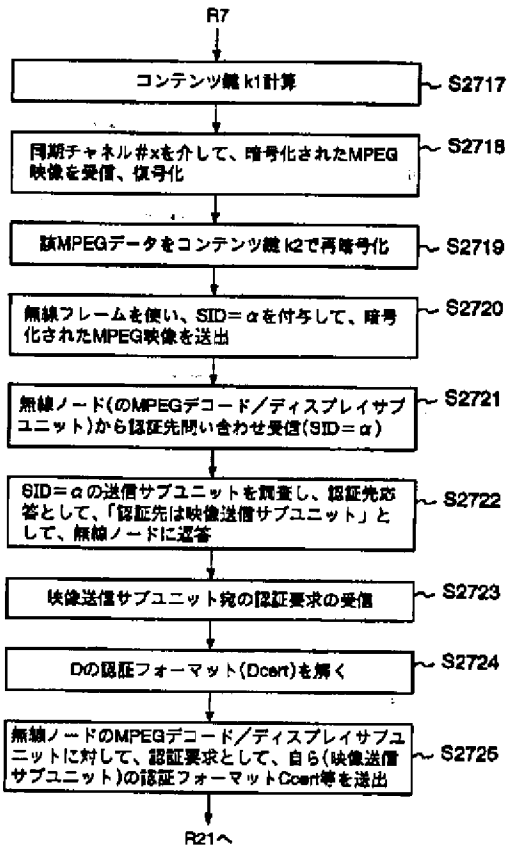
【図28】


スタート
無線ノード構成情報の受信(無線ノードが認証フォーマットを持つことを確認)
S2701
無線ノードの構成(サブユニット情報)を、自己(中継ノード)のサブユニットとして代理構成。対応関係を代理テーブルに登録
S2702
上記代理サブユニット構成を外部に広告(IEEE1212レジスタ、AV/Cプロトコル等を通して)。認証フォーマットを持つものとして広告
S2703
AV/Cコマンドの受信(MPEGデコード/ディスプレイサブユニットに同期チャネル#xからのストリームを入力せよ)
S2704
代理テーブルを参照
S2705
無線区間のQOSを確保
S2706
ISO信号送受信部(同期チャネル#xを受信)2203と、無線ISO信号送受信部2206を接続。1394/Fからの入力信号を無線区間へ出力できるようにする
S2707
無線ノードに対して、無線ノード制御パケットを送信
S2708
R6へ

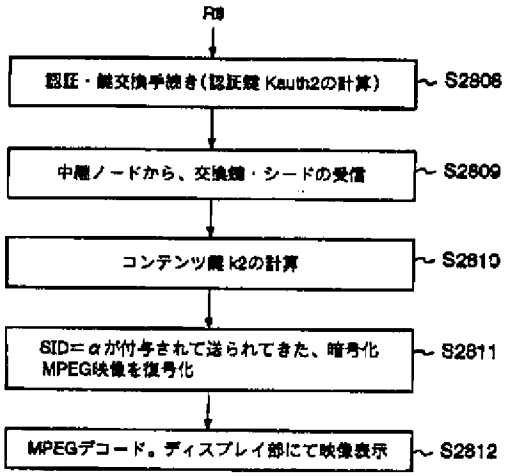
【図29】



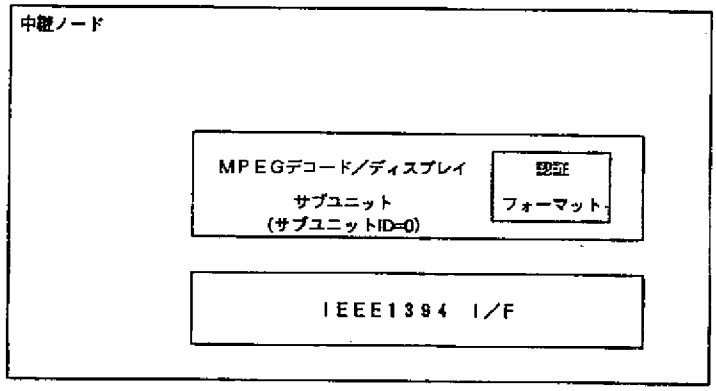
【図30】



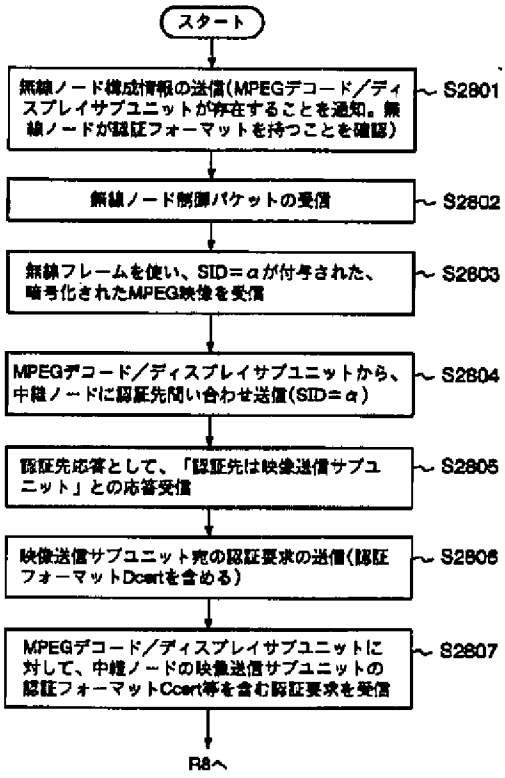
【図33】



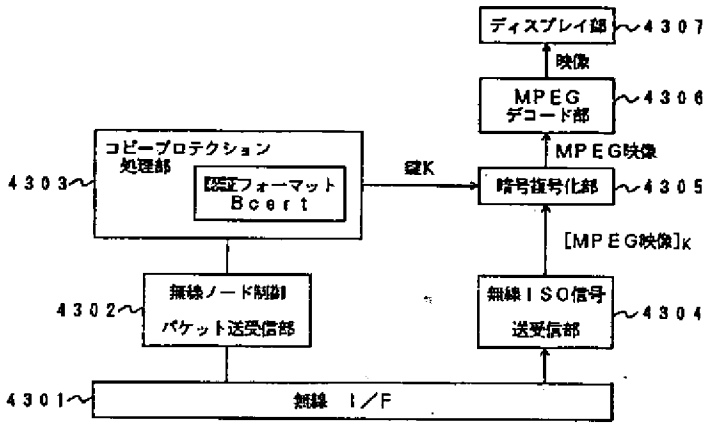
【図36】



【図３２】



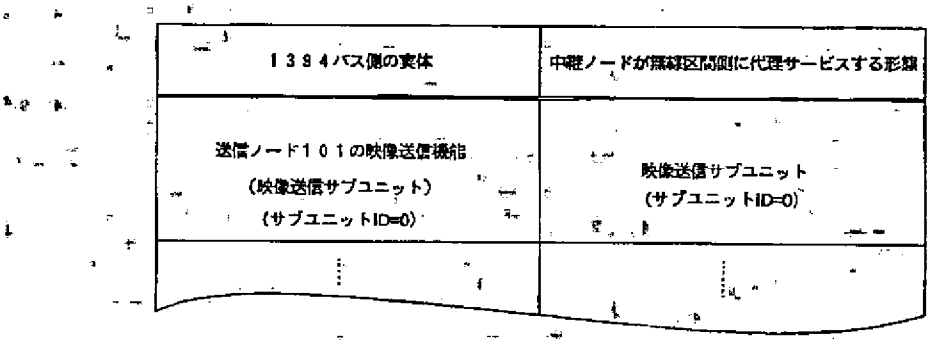
【図４３】



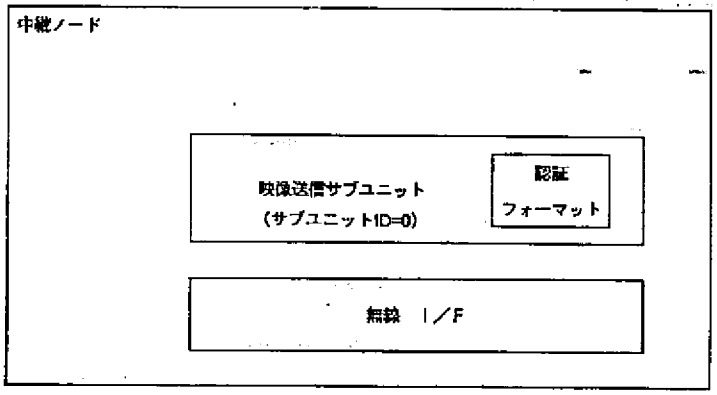
【図３４】

無線区間側の実体	中継ノードが１３９４側に代理サービスする形態
無線ノード１０３の ＭＰＥＧデコード/ディスプレイ機能 （サブユニットID=0）	ＭＰＥＧデコード/ディスプレイサブユニット （サブユニットID=0）
⋮	⋮

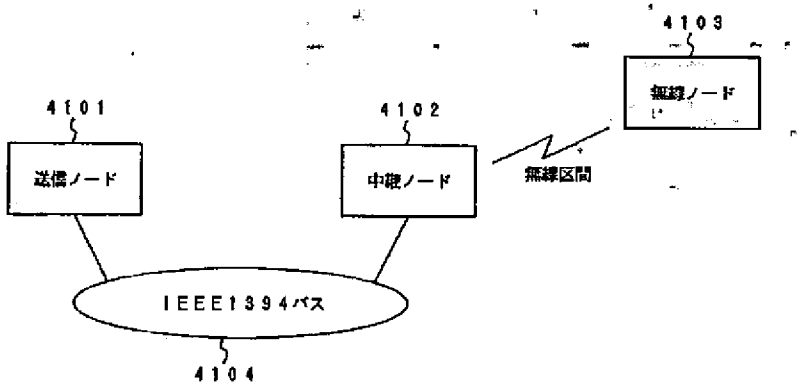
【図35】


1394バス側の実体
中継ノードが無線区間側に代理サービスする形態
送信ノード101の映像送信機能
(映像送信サブユニット)
(サブユニットID=0)
映像送信サブユニット
(サブユニットID=0)

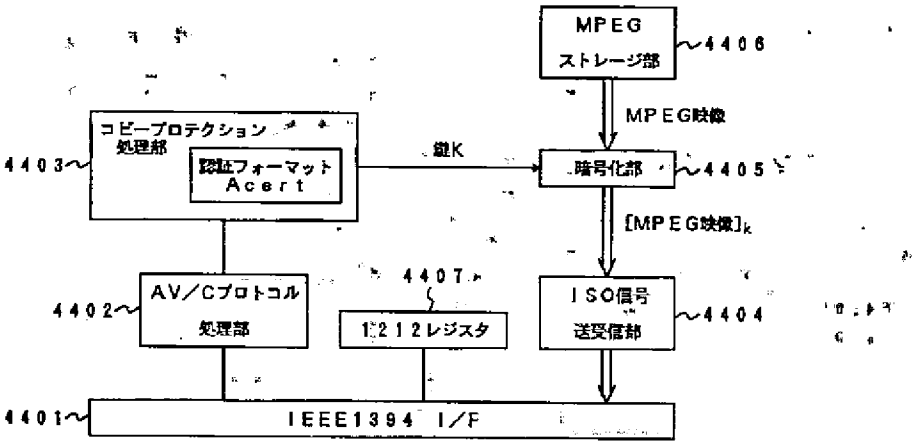
【図37】


中継ノード
映像送信サブユニット
(サブユニットID=0)
認証
フォーマット
無線 I/F

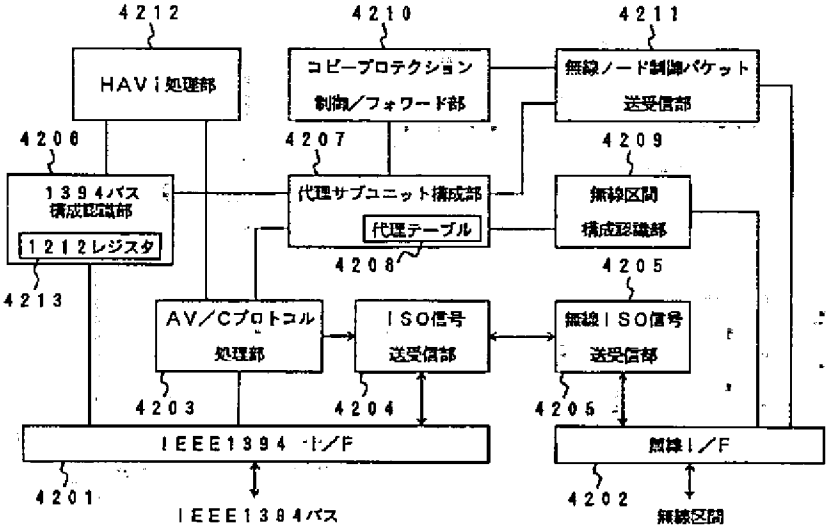
【図40】


4103
無線ノード
4101
送信ノード
4102
中継ノード
無線区間
IEEE1394バス
4104

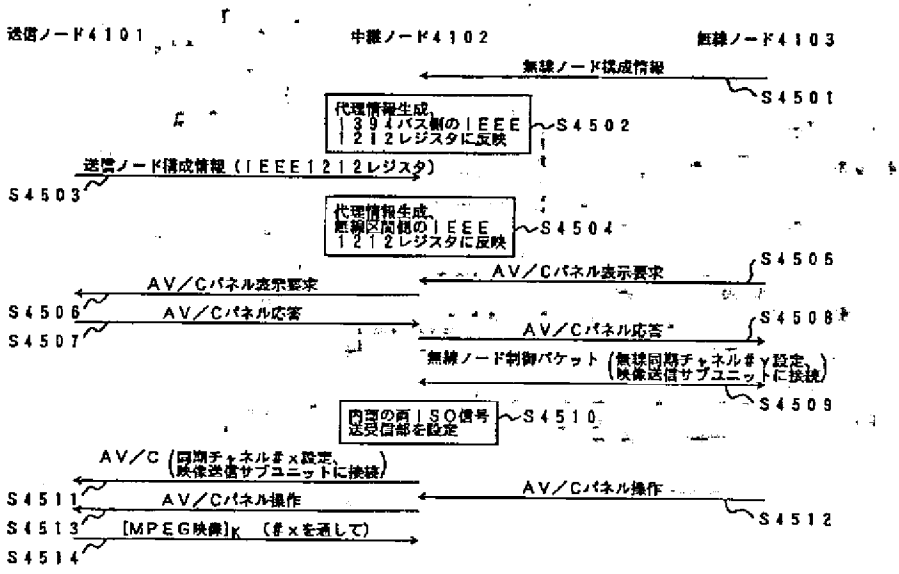
【図41】


MPEG
ストレージ部
4406
MPEG映像
コピープロテクション
処理部
4403
認証フォーマット
Acert
鍵K
暗号化部
4405
[MPEG映像]k
4407
AV/Cプロトコル
処理部
4402
1212レジスタ
ISO信号
送受信部
4404
4401
IEEE1394 I/F

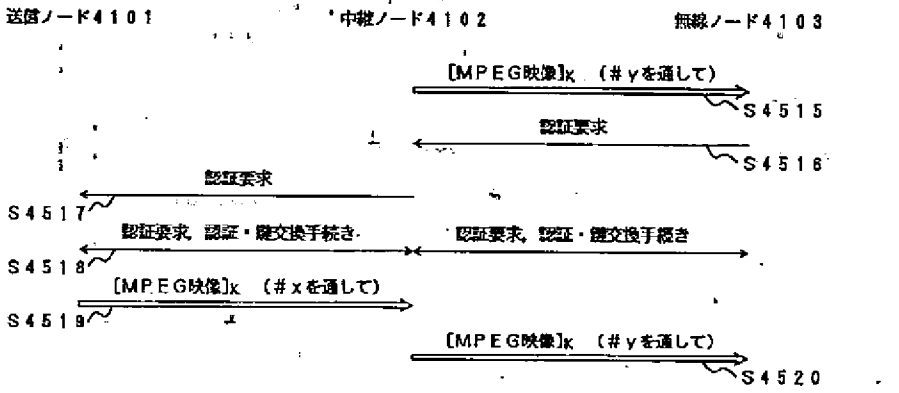
【図42】


4212
4210
4211
HAVi処理部
コピープロテクション
制御/フォワード部
無線ノード制御パケット
送受信部
4206
4207
4209
1394バス
構成認識部
1212レジスタ
4213
代理サブユニット構成部
代理テーブル
4208
無線区間
構成認識部
4205
AV/Cプロトコル
処理部
ISO信号
送受信部
無線ISO信号
送受信部
4203
4204
4205
IEEE1394 I/F
無線I/F
4201
4202
IEEE1394バス
無線区間

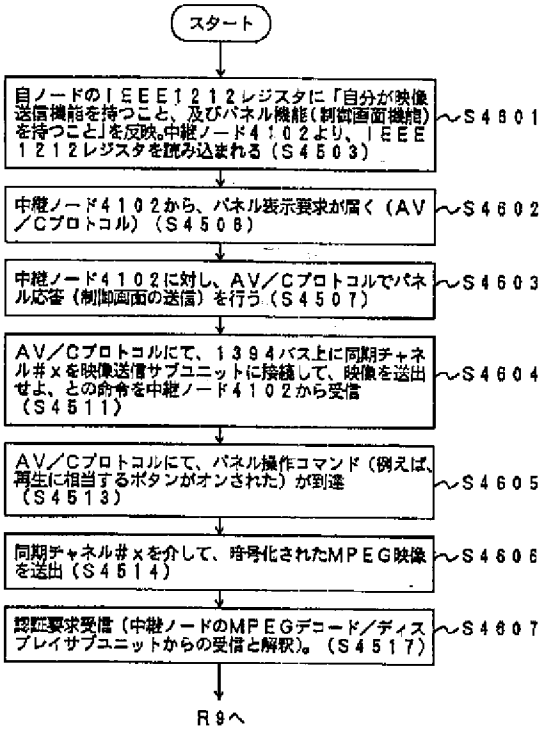
【図44】


送信ノード4101
中継ノード4102
無線ノード4103
無線ノード構成情報
S4501
代理情報生成、
1394バス側のIEEE
1212レジスタに反映
S4502
送信ノード構成情報（IEEE1212レジスタ）
S4503
代理情報生成、
無線区間側のIEEE
1212レジスタに反映
S4504
S4505
AV/Cパネル表示要求
AV/Cパネル表示要求
S4506
AV/Cパネル応答
AV/Cパネル応答
S4508
S4507
無線ノード制御パケット（無線同期チャネル#y設定、映像送信サブユニットに接続）
S4509
同期の両ISO信号送受信部を設定
S4510
AV/C（同期チャネル#x設定、映像送信サブユニットに接続）
AV/Cパネル操作
AV/Cパネル操作
S4511
S4512
S4513
[MPEG映像]K （#xを通して）
S4514

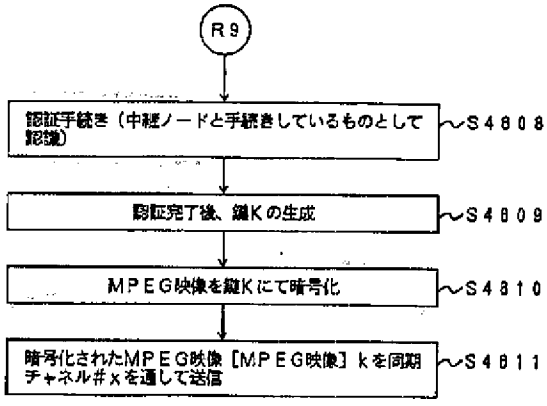
【図45】


送信ノード4101
中継ノード4102
無線ノード4103
[MPEG映像]K （#yを通して）
S4515
認証要求
S4516
認証要求
S4517
認証要求、認証・鍵交換手続き
認証要求、認証・鍵交換手続き
S4518
[MPEG映像]K （#xを通して）
S4519
[MPEG映像]K （#yを通して）
S4520

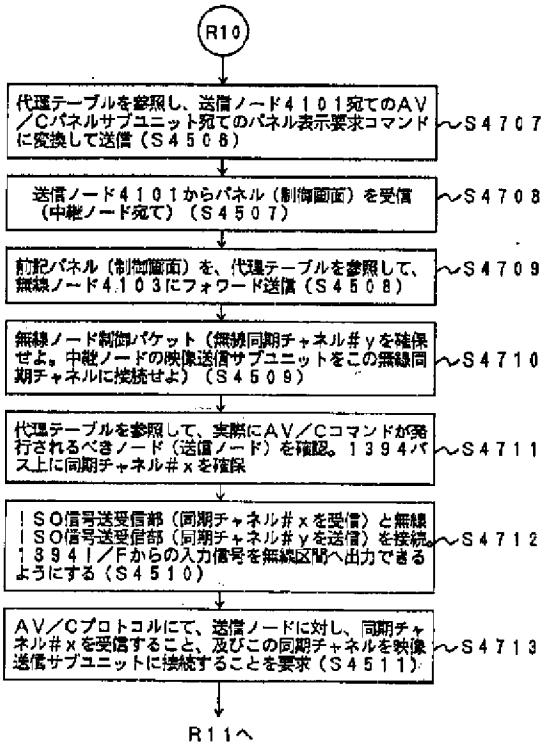
【図46】



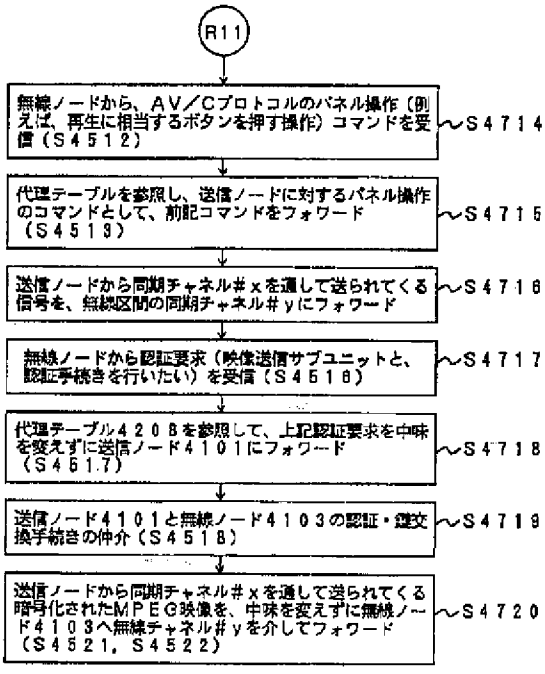
【図47】



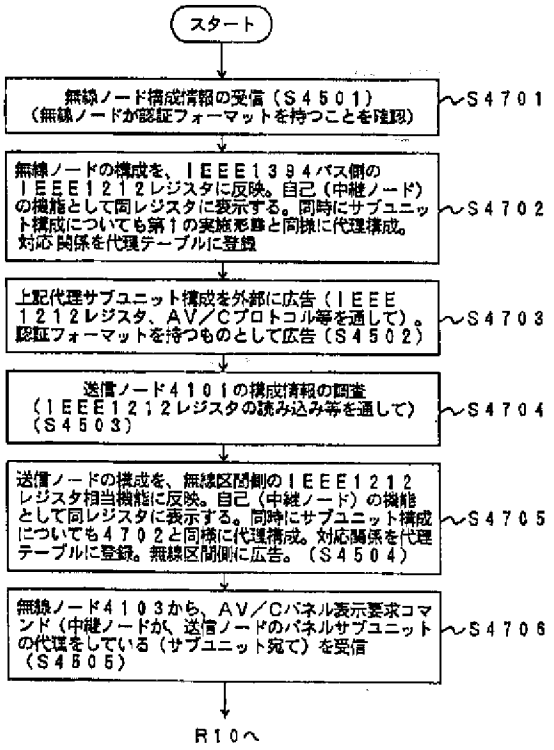
【図49】



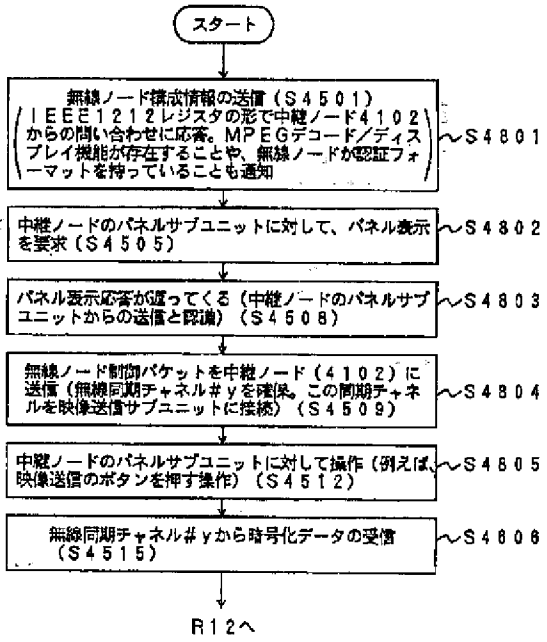
【図50】



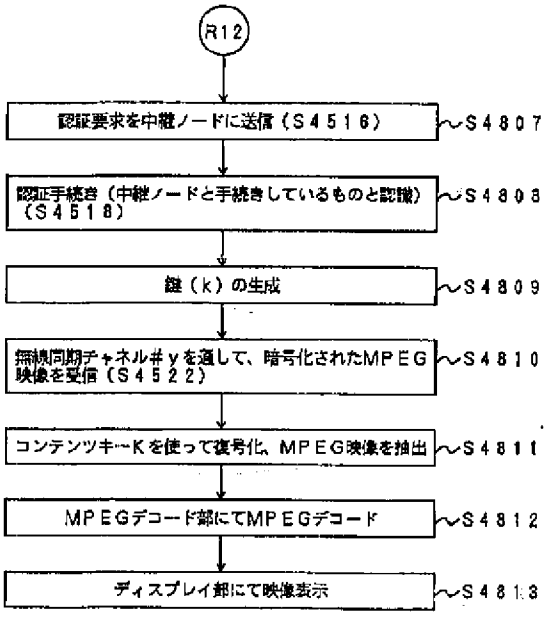
【図48】



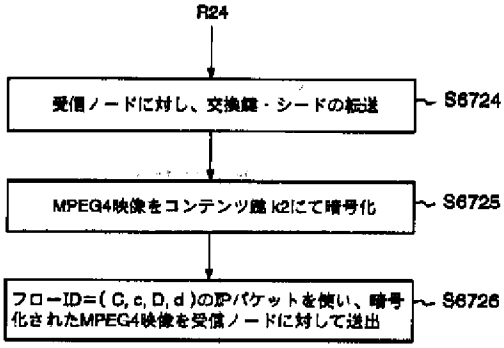
【図51】



【図52】



【図69】



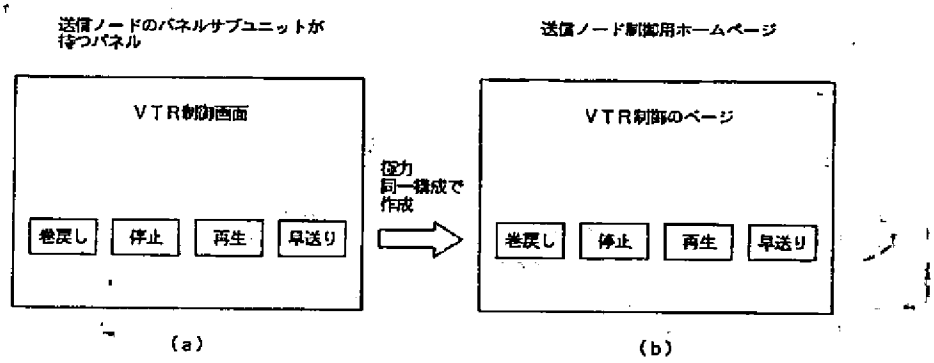
【図53】

無線区間側の実体	中継ノードが1394側に代理サービスする形態
無線ノード4103の MPEGデコード/ディスプレイ機能 (認証フォーマット有)	MPEGデコード/ディスプレイサブユニット (認証フォーマット有)
無線ノード4103のパネル機能	パネルサブユニット

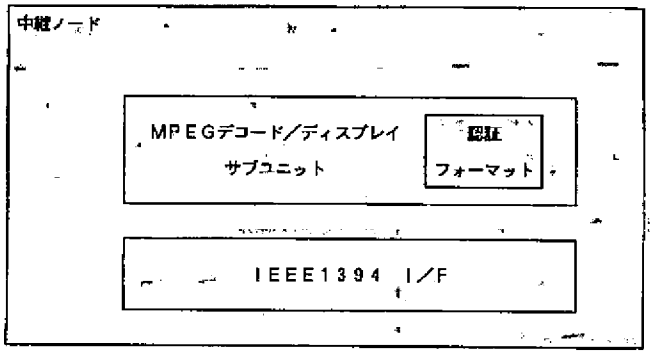
【図54】

1394バス側の実体	中継ノードが無線区間側に代理サービスする形態
送信ノード4101の映像送信サブユニット (認証フォーマット有)	映像送信サブユニット (認証フォーマット有)
送信ノード4101のパネルサブユニット	パネルサブユニット

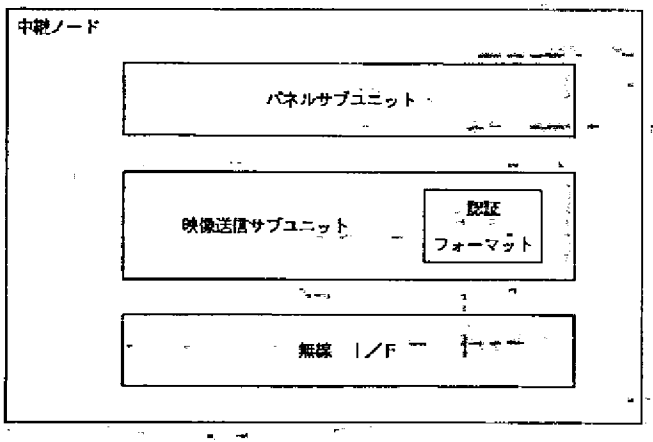
【図72】



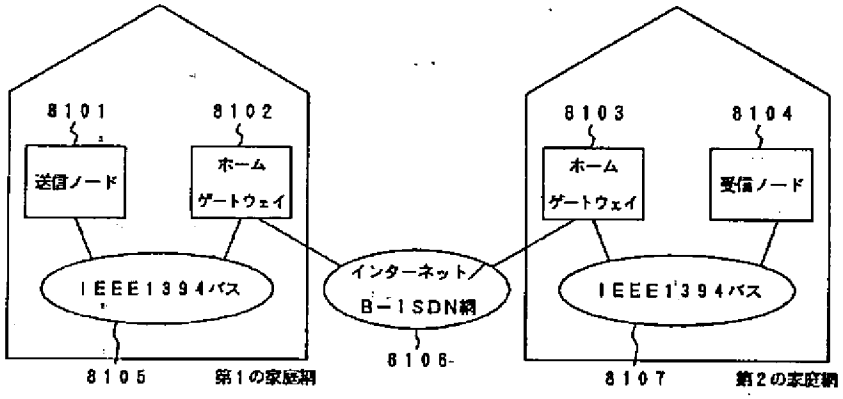
【図55】


中継ノード
MPEGデコード/ディスプレイ
サブユニット
認証
フォーマット
IEEE1394 I/F

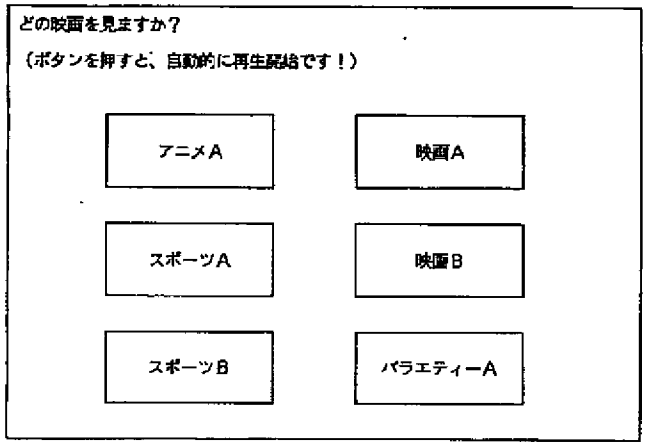
【図56】


中継ノード
パネルサブユニット
映像送信サブユニット
認証
フォーマット
無線 I/F

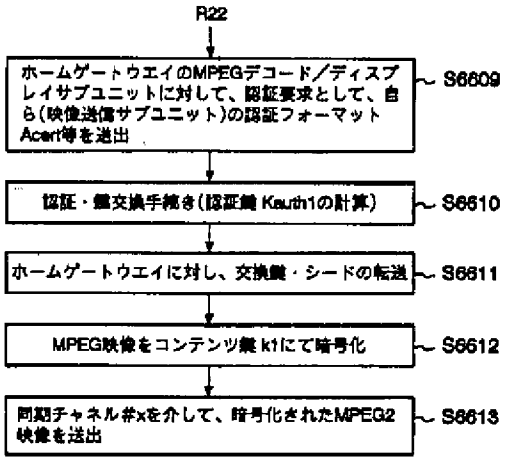
【図73】


8101
8102
送信ノード
ホーム
ゲートウェイ
IEEE1394バス
8105
第1の家庭網
インターネット/
B-ISDN網
8106
8103
8104
ホーム
ゲートウェイ
受信ノード
IEEE1394バス
8107
第2の家庭網

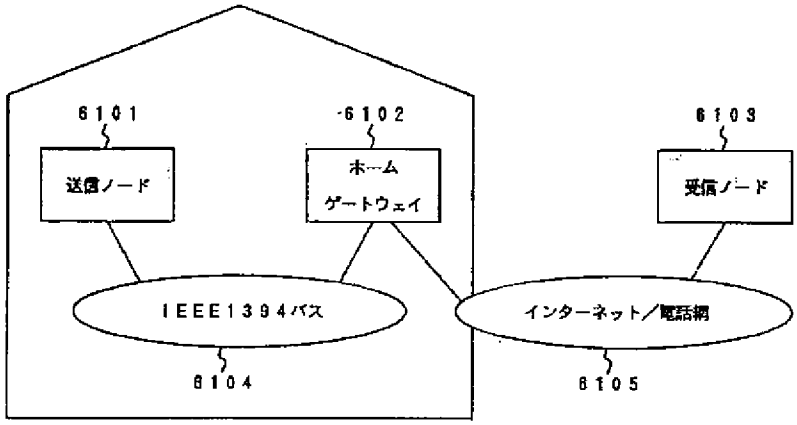
【図57】


どの映画を見ますか？
（ボタンを押すと、自動的に再生開始です！）
アニメA
映画A
スポーツA
映画B
スポーツB
バラエティーA

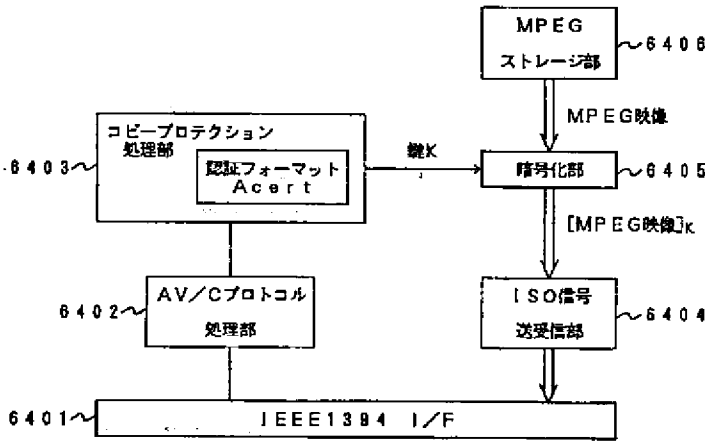
【図65】


R22
ホームゲートウエイのMPEGデコード／ディスプレイサブユニットに対して、認証要求として、自ら（映像送信サブユニット）の認証フォーマットAcert等を送出
S6609
認証・鍵交換手続き（認証鍵 Kauth1の計算）
S6610
ホームゲートウエイに対し、交換鍵・シードの転送
S6611
MPEG映像をコンテンツ鍵 k1にて暗号化
S6612
同期チャネル#xを介して、暗号化されたMPEG2映像を送出
S6613

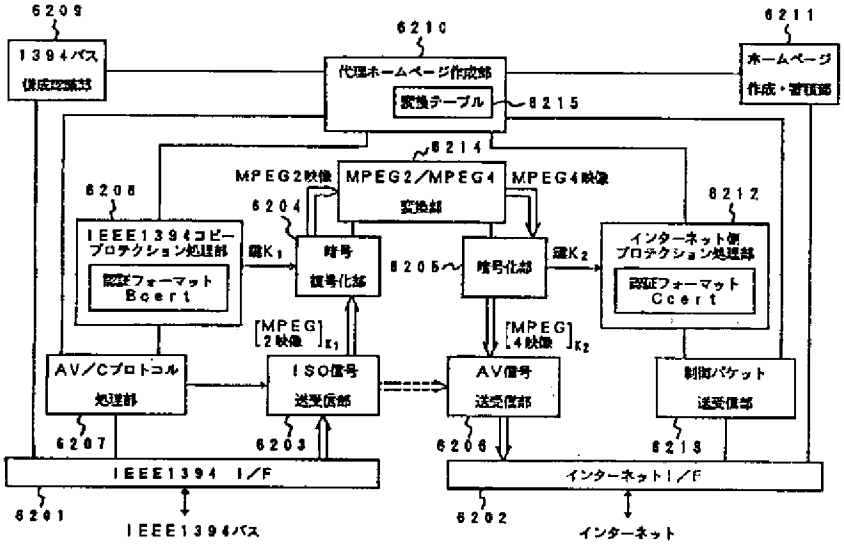
【図58】


6101
送信ノード
6102
ホーム
ゲートウェイ
6103
受信ノード
IEEE1394バス
6104
インターネット／電話網
6105

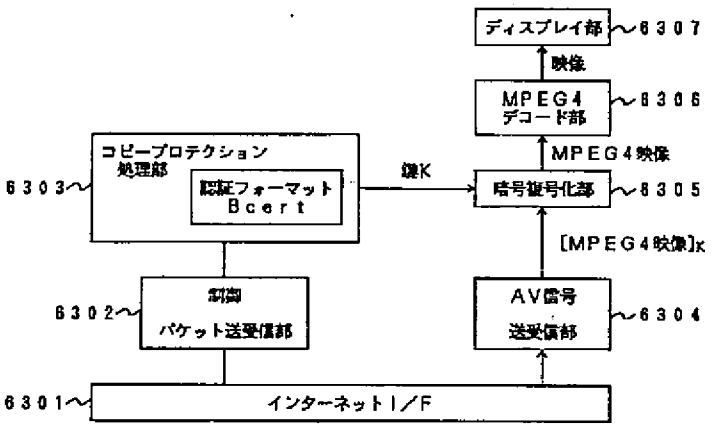
【図59】


MPEG
ストレージ部
6406
MPEG映像
コピープロテクション
処理部
認証フォーマット
Acert
6403
鍵K
暗号化部
6405
[MPEG映像]K
AV/Cプロトコル
処理部
6402
ISO信号
送受信部
6404
6401
IEEE1394 I/F

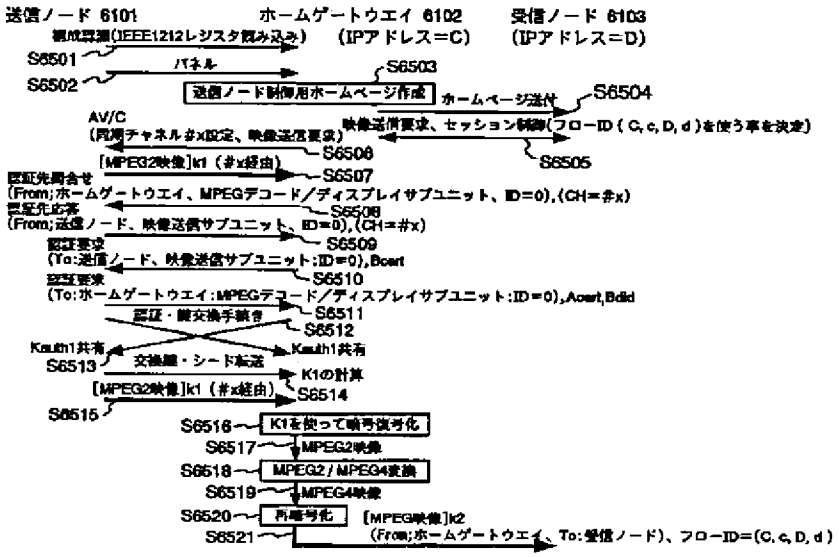
【図60】


6209
1394バス
6210
代理ホームページ作成部
変換テーブル
6215
6211
ホームページ
作成・管理部
6214
MPEG2映像
MPEG2/MPEG4
変換部
MPEG4映像
6208
6204
6212
IEEE1394コピー
プロテクション処理部
認証フォーマット
Bcert
鍵K1
暗号
復号化部
6205
暗号化部
鍵K2
インターネット側
プロテクション処理部
認証フォーマット
Ccert
[MPEG
2映像]K1
[MPEG
4映像]K2
AV/Cプロトコル
処理部
ISO信号
送受信部
AV信号
送受信部
制御パケット
送受信部
6207
6203
6216
6218
IEEE1394 I/F
インターネットI/F
6201
6202
IEEE1394バス
インターネット

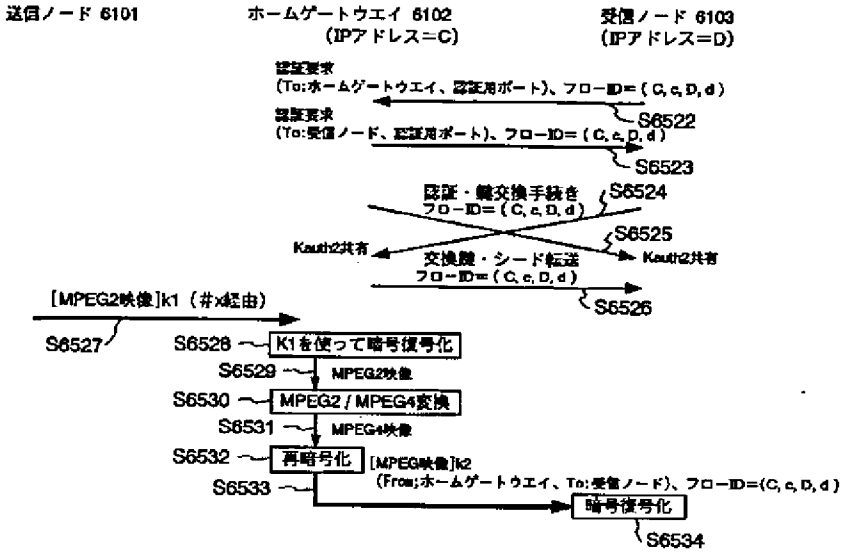
【図61】


ディスプレイ部
6307
映像
MPEG4
デコード部
6306
MPEG4映像
コピープロテクション
処理部
6303
認証フォーマット
Bcert
鍵K
暗号復号化部
6305
[MPEG4映像]K
制御
パケット送受信部
6302
AV信号
送受信部
6304
6301
インターネットI/F

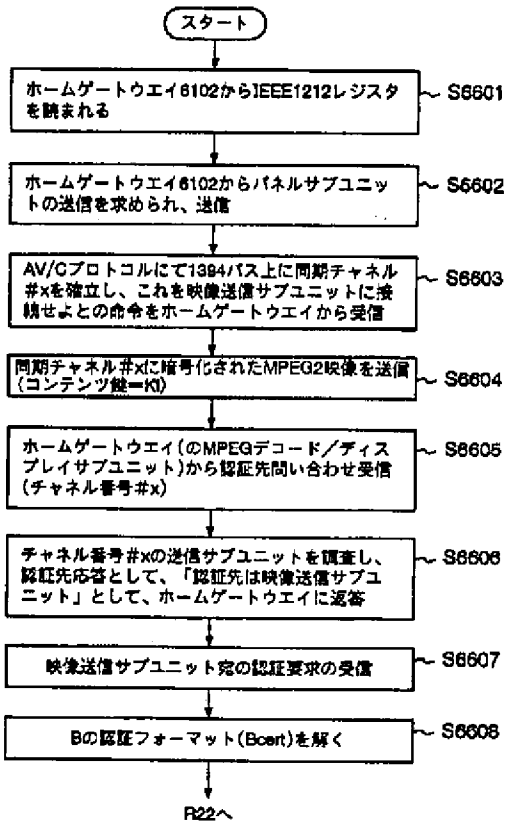
【図62】


送信ノード 6101
ホームゲートウエイ 6102
(IPアドレス=C)
受信ノード 6103
(IPアドレス=D)
S6501
S6502
パネル
S6503
送信ノード制御用ホームページ作成
ホームページ送付
S6504
AV/C
S6505
S6506
[MPEG2映像]k1 (#x経由)
S6507
(From;ホームゲートウエイ、MPEGデコード/ディスプレイサブユニット、ID=0),(CH=#x)
S6508
(From;送信ノード、映像送信サブユニット、ID=0),(CH=#x)
S6509
(To:送信ノード、映像送信サブユニット:ID=0),Bcert
S6510
(To:ホームゲートウエイ:MPEGデコード/ディスプレイサブユニット:ID=0),Acert,Bdid
認証・鍵交換手続き
S6511
S6512
Kauth1共有
S6513
交換鍵・シード転送
K1の計算
[MPEG2映像]k1 (#x経由)
S6514
S6515
S6516
K1を使って暗号復号化
S6517
MPEG2映像
S6518
MPEG2/MPEG4変換
S6519
MPEG4映像
S6520
S6521
[MPEG映像]k2
(From;ホームゲートウエイ、To:受信ノード)、フローID=(C, c, D, d)

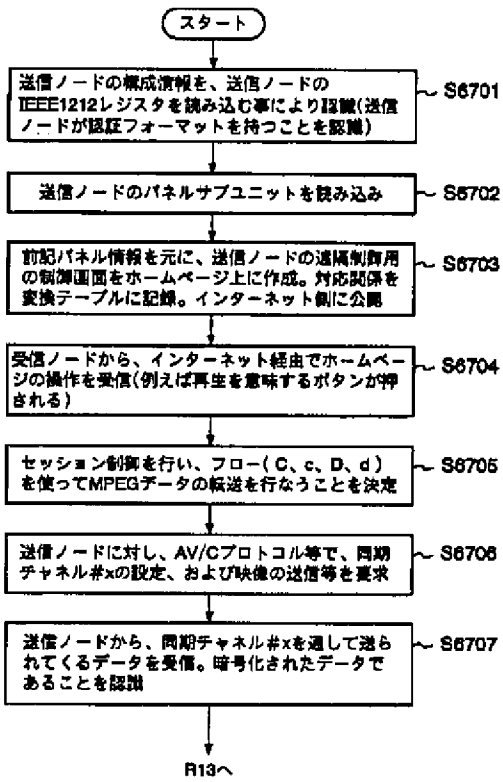
【図63】


送信ノード 6101
ホームゲートウエイ 6102
(IPアドレス=C)
受信ノード 6103
(IPアドレス=D)
認証要求
(To:ホームゲートウエイ、認証用ポート)、フローID=(C, c, D, d)
S6522
認証要求
(To:受信ノード、認証用ポート)、フローID=(C, c, D, d)
S6523
認証・鍵交換手続き
フローID=(C, c, D, d)
S6524
S6525
Kauth2共有
Kauth2共有
交換鍵・シード転送
フローID=(C, c, D, d)
S6526
[MPEG2映像]k1 (#x経由)
S6527
S6528
K1を使って暗号復号化
S6529
MPEG2映像
S6530
MPEG2 / MPEG4変換
S6531
MPEG4映像
S6532
再暗号化
[MPEG映像]k2
(From:ホームゲートウエイ、To:受信ノード)、フローID=(C, c, D, d)
S6533
暗号復号化
S6534

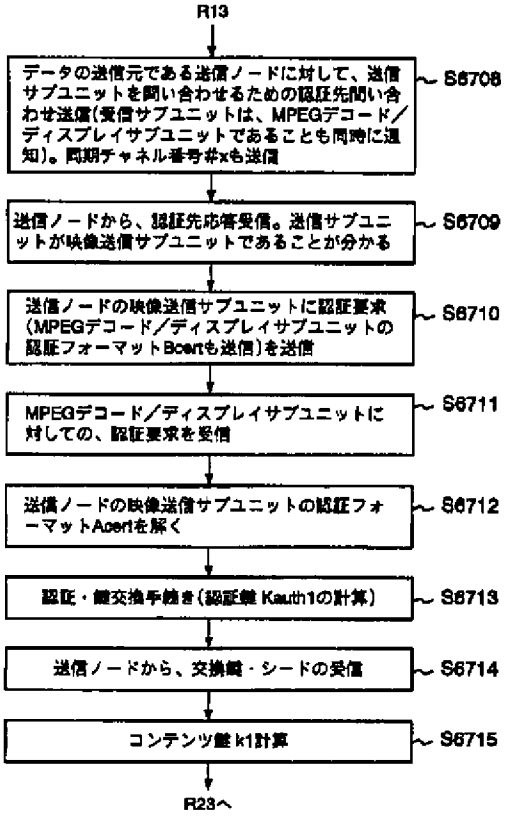
【図64】


スタート
ホームゲートウエイ6102からIEEE1212レジスタを読まれる
S6601
ホームゲートウエイ6102からパネルサブユニットの送信を求められ、送信
S6602
AV/Cプロトコルにて1394バス上に同期チャネル#xを確立し、これを映像送信サブユニットに接続せよとの命令をホームゲートウエイから受信
S6603
同期チャネル#xに暗号化されたMPEG2映像を送信(コンテンツ鍵=K)
S6604
ホームゲートウエイ(のMPEGデコード/ディスプレイサブユニット)から認証先問い合わせ受信(チャネル番号#x)
S6605
チャネル番号#xの送信サブユニットを調査し、認証先応答として、「認証先は映像送信サブユニット」として、ホームゲートウエイに返答
S6606
映像送信サブユニット宛の認証要求の受信
S6607
Bの認証フォーマット(Bcert)を解く
S6608
R22へ

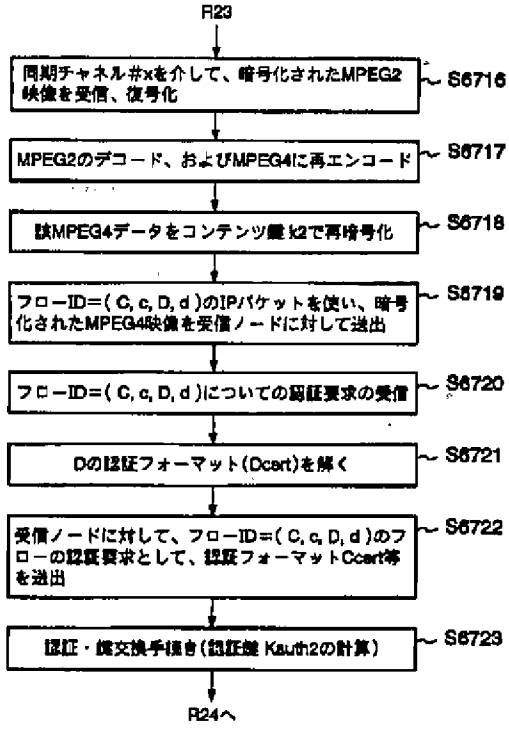
【図66】


スタート
送信ノードの構成情報を、送信ノードのIEEE1212レジスタを読み込む事により認識(送信ノードが認証フォーマットを持つことを認識)
S6701
送信ノードのパネルサブユニットを読み込み
S6702
前記パネル情報を元に、送信ノードの遠隔制御用の制御画面をホームページ上に作成。対応関係を変換テーブルに記録。インターネット側に公開
S6703
受信ノードから、インターネット経由でホームページの操作を受信(例えば再生を意味するボタンが押される)
S6704
セッション制御を行い、フロー(C、c、D、d)を使ってMPEGデータの転送を行なうことを決定
S6705
送信ノードに対し、AV/Cプロトコル等で、同期チャネル#xの設定、および映像の送信等を要求
S6706
送信ノードから、同期チャネル#xを通して送られてくるデータを受信。暗号化されたデータであることを認識
S6707
R13へ

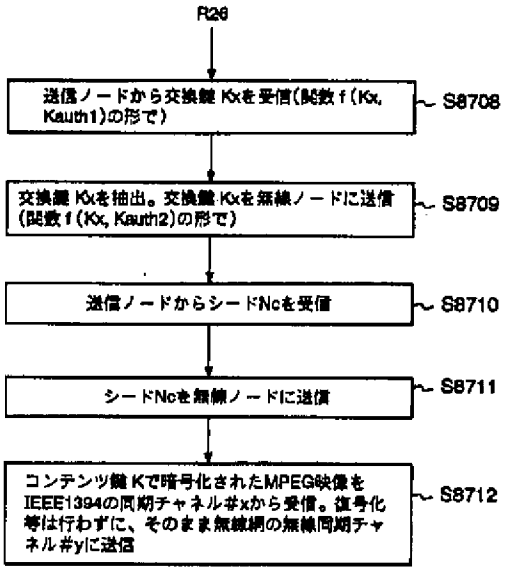
【図67】



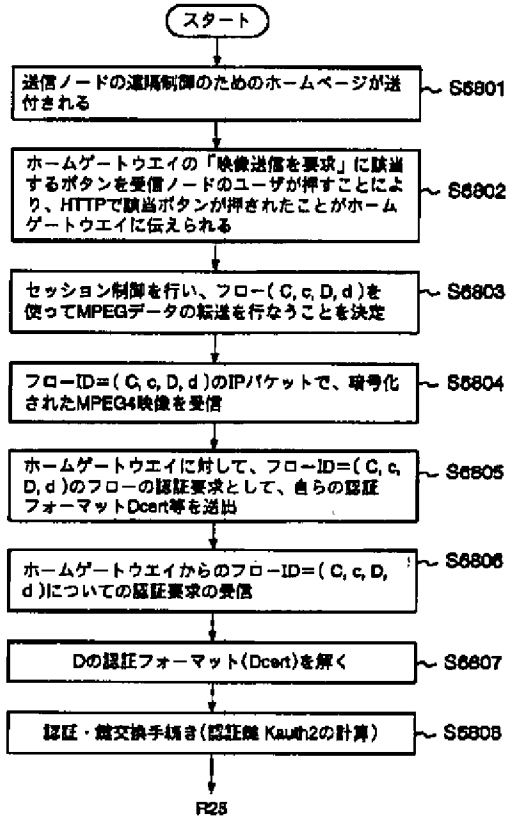
【図68】



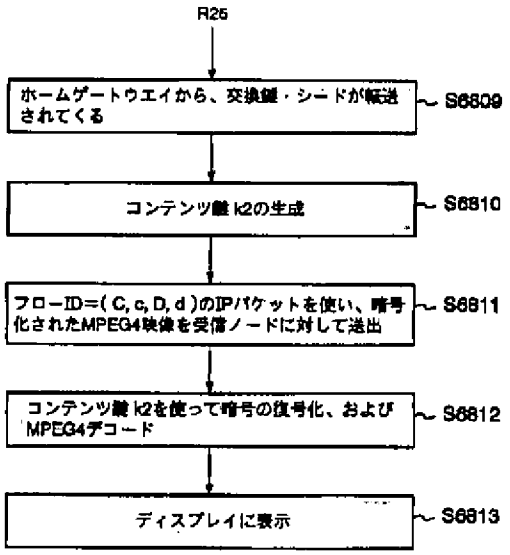
【図84】



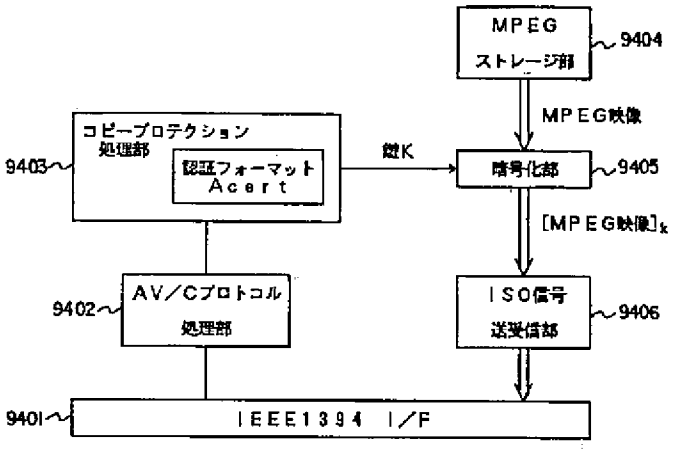
【図70】



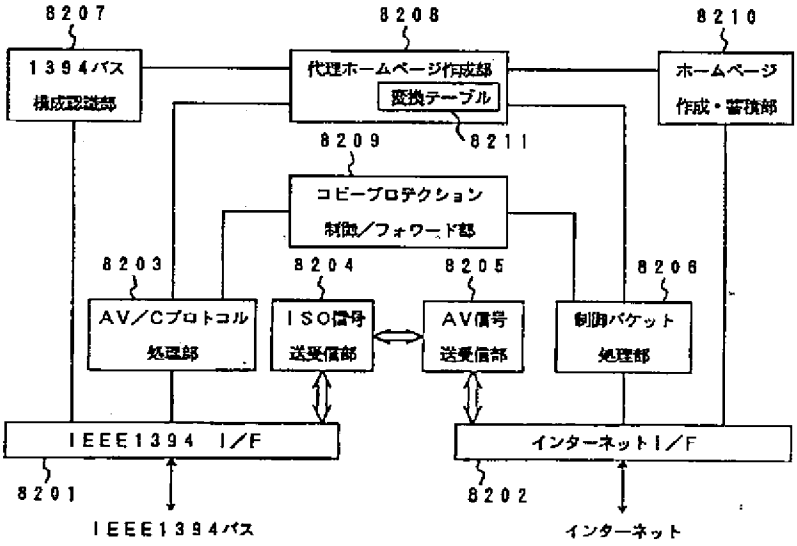
【図71】


R25
ホームゲートウエイから、交換鍵・シードが転送されてくる
S6809
コンテンツ鍵k2の生成
S6810
フローID=(C, c, D, d)のIPパケットを使い、暗号化されたMPEG4映像を受信ノードに対して送出
S6811
コンテンツ鍵k2を使って暗号の復号化、およびMPEG4デコード
S6812
ディスプレイに表示
S6813

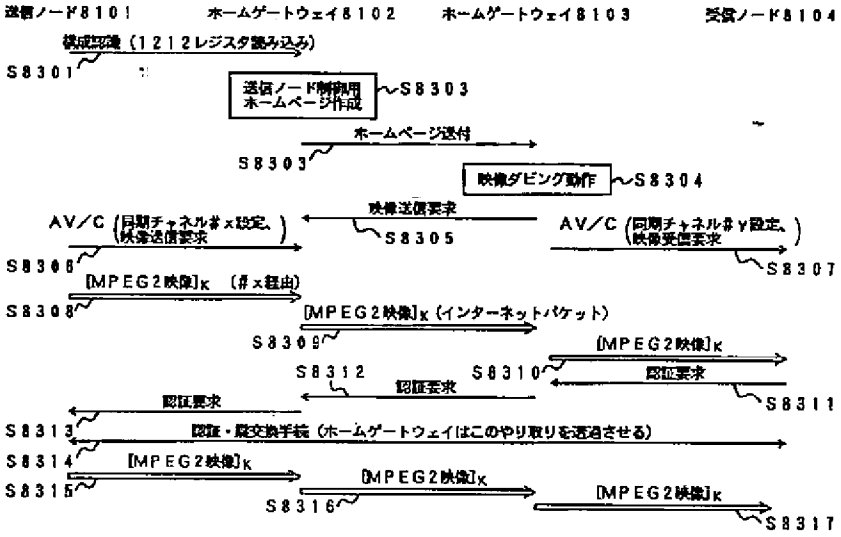
【図78】


MPEG
ストレージ部
9404
MPEG映像
コピープロテクション
処理部
認証フォーマット
Acert
9403
鍵K
暗号化部
9405
[MPEG映像]k
AV/Cプロトコル
処理部
9402
ISO信号
送受信部
9406
IEEE1394 I/F
9401

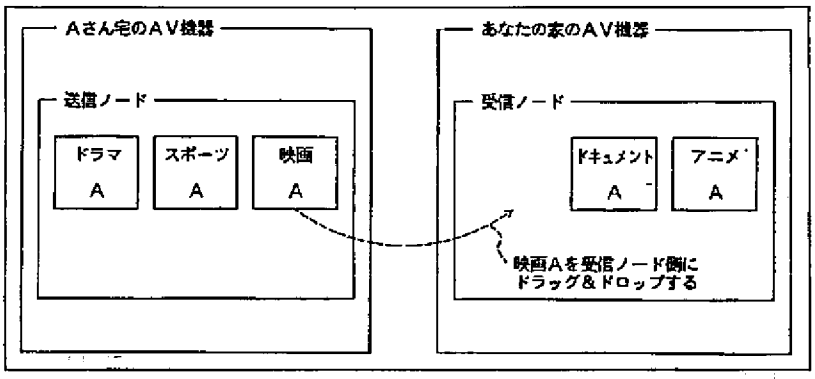
【図74】


8207
1394バス
構成認識部
8208
代理ホームページ作成部
変換テーブル
8211
8210
ホームページ
作成・蓄積部
8209
コピープロテクション
制御/フォワード部
8203
AV/Cプロトコル
処理部
8204
ISO信号
送受信部
8205
AV信号
送受信部
8206
制御パケット
処理部
IEEE1394 I/F
8201
IEEE1394バス
インターネットI/F
8202
インターネット

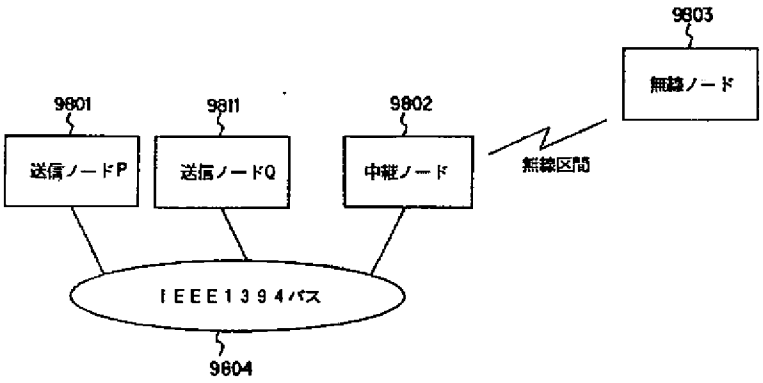
【図75】


送信ノード8101
ホームゲートウェイ8102
ホームゲートウェイ8103
受信ノード8104
構成取得（1212レジスタ読み込み）
S8301
送信ノード制御用ホームページ作成
S8303
ホームページ送付
S8303
映像ダビング動作
S8304
映像送信要求
S8305
AV/C（同期チャネル#x設定、映像送信要求）
AV/C（同期チャネル#y設定、映像受信要求）
S8306
S8307
[MPEG2映像]K （#x経由）
S8308
[MPEG2映像]K（インターネットパケット）
S8309
[MPEG2映像]K
S8310
認証要求
S8311
S8312
認証要求
認証要求
S8313
認証・暗号交換手続（ホームゲートウェイはこのやり取りを透過させる）
S8314
[MPEG2映像]K
S8315
[MPEG2映像]K
S8316
[MPEG2映像]K
S8317

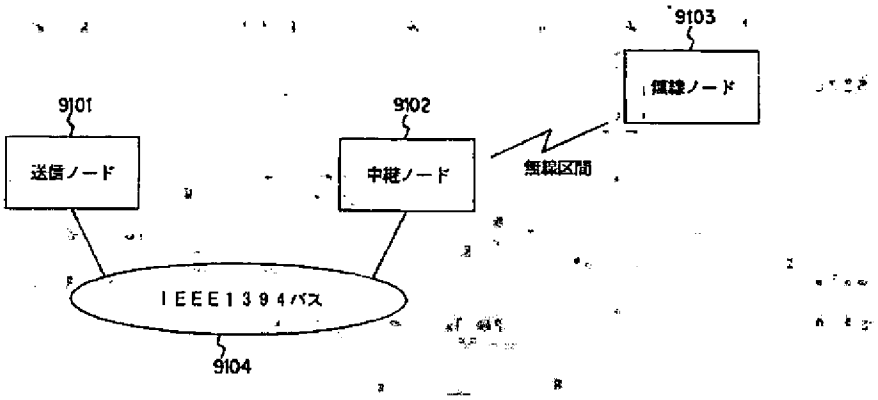
【図76】


Aさん宅のAV機器
送信ノード
ドラマ A
スポーツ A
映画 A
あなたの家のAV機器
受信ノード
ドキュメント A
アニメ A
映画Aを受信ノード側にドラッグ&ドロップする

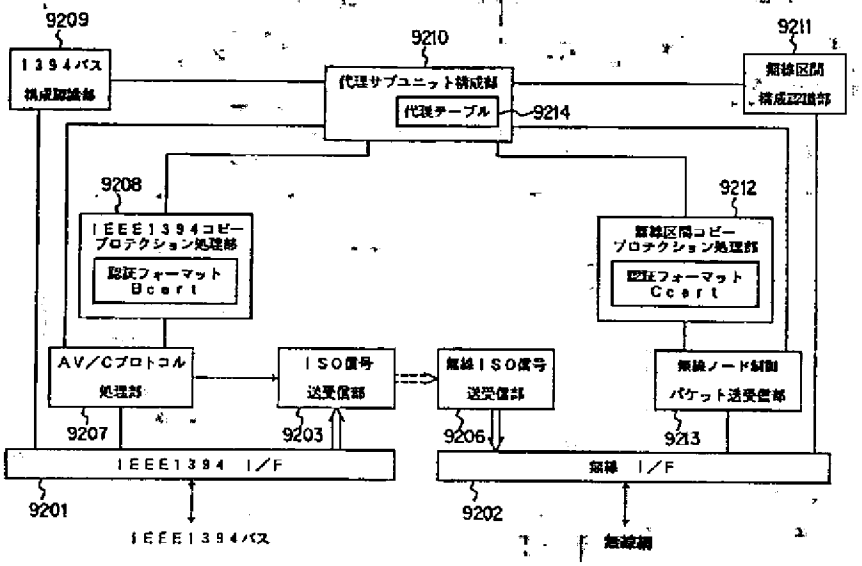
【図87】


9803
無線ノード
9801
送信ノードP
9811
送信ノードQ
9802
中継ノード
無線区間
IEEE1394バス
9804

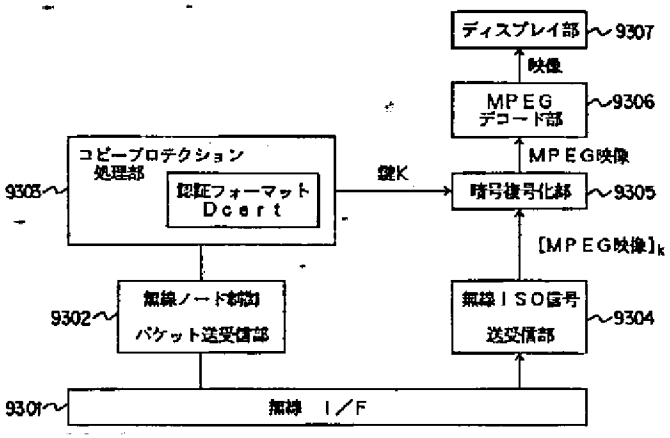
【図77】


9103
無線ノード
9101
送信ノード
9102
中継ノード
無線区間
IEEE1394バス
9104

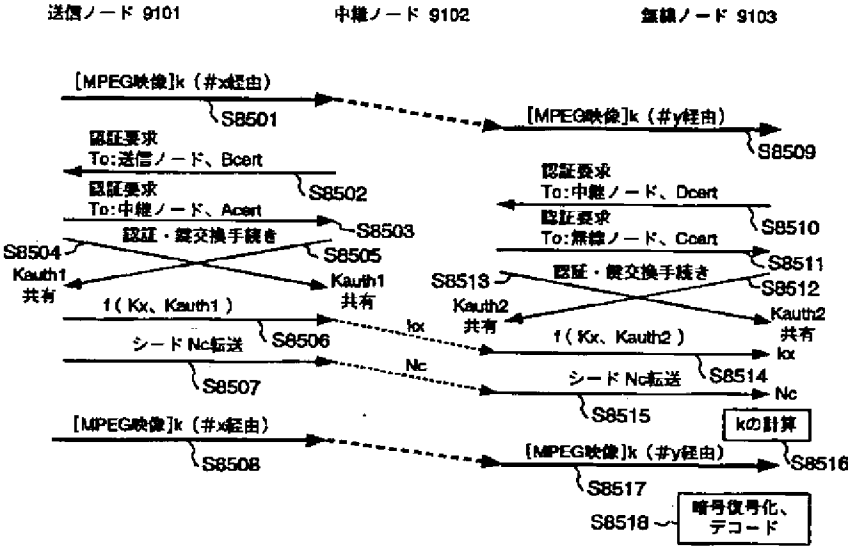
【図79】


9209
1394バス
構成認識部
9210
代理サブユニット構成部
代理テーブル
9214
9211
無線区間
構成認識部
9208
IEEE1394コピー
プロテクション処理部
認証フォーマット
Bcert
9212
無線区間コピー
プロテクション処理部
認証フォーマット
Ccert
AV/Cプロトコル
処理部
ISO信号
送受信部
無線ISO信号
送受信部
無線ノード制御
パケット送受信部
9207
9203
9206
9213
IEEE1394 I/F
無線 I/F
9201
9202
IEEE1394バス
無線網

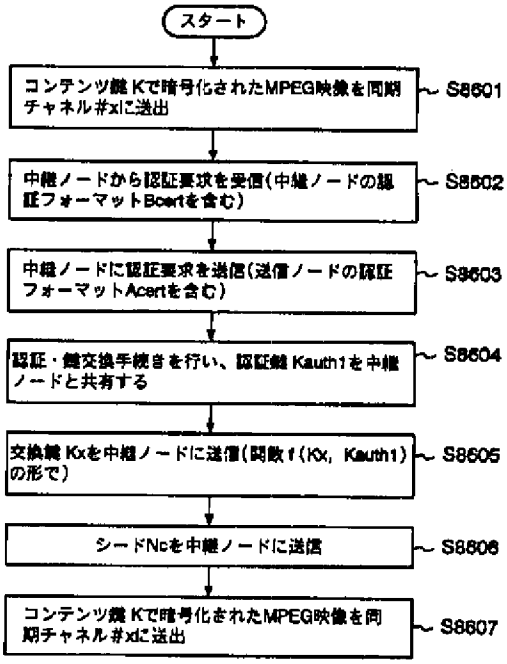
【図８０】


ディスプレイ部
9307
映像
MPEG
デコード部
9306
MPEG映像
コピープロテクション
処理部
認証フォーマット
Dcert
9303
鍵K
暗号復号化部
9305
[MPEG映像]k
無線ノード制御
パケット送受信部
9302
無線ISO信号
送受信部
9304
9301
無線 I／F

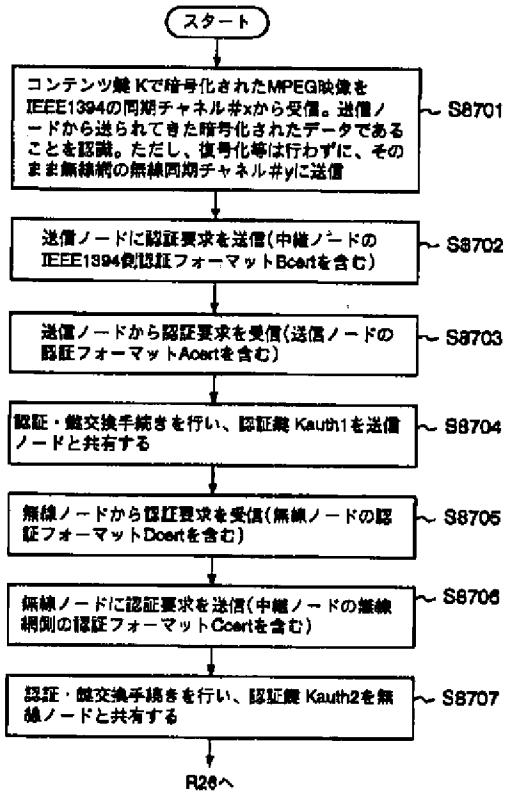
【図８１】


送信ノード 9101
中継ノード 9102
無線ノード 9103
[MPEG映像]k（#x経由）
S8501
[MPEG映像]k（#y経由）
S8509
認証要求
To:送信ノード、Bcert
S8502
認証要求
To:中継ノード、Acert
S8503
認証・鍵交換手続き
S8504
S8505
Kauth1
共有
Kauth1
共有
f（Kx、Kauth1）
S8506
シードNc転送
S8507
Nc
[MPEG映像]k（#x経由）
S8508
認証要求
To:中継ノード、Dcert
S8510
認証要求
To:無線ノード、Ccert
S8511
S8513
認証・鍵交換手続き
S8512
Kauth2
共有
Kauth2
共有
f（Kx、Kauth2）
kx
S8514
シードNc転送
Nc
S8515
kの計算
S8516
[MPEG映像]k（#y経由）
S8517
S8518
暗号復号化、
デコード

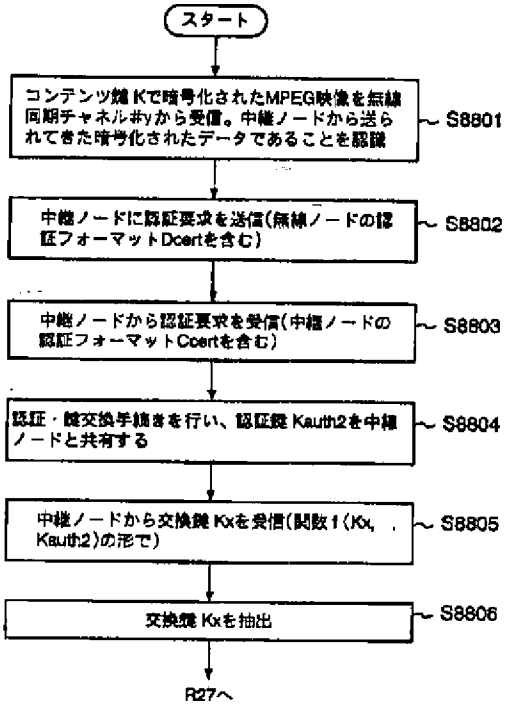
【図８２】


スタート
コンテンツ鍵Kで暗号化されたMPEG映像を同期チャネル#xに送出
S8601
中継ノードから認証要求を受信(中継ノードの認証フォーマットBcertを含む)
S8602
中継ノードに認証要求を送信(送信ノードの認証フォーマットAcertを含む)
S8603
認証・鍵交換手続きを行い、認証鍵Kauth1を中継ノードと共有する
S8604
交換鍵Kxを中継ノードに送信(関数f(Kx, Kauth1)の形で)
S8605
シードNcを中継ノードに送信
S8606
コンテンツ鍵Kで暗号化されたMPEG映像を同期チャネル#xdに送出
S8607

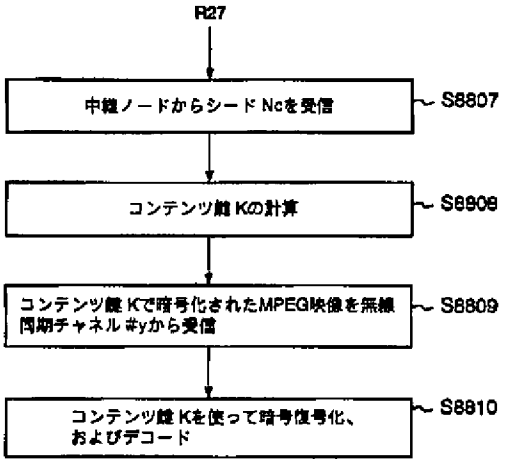
【図８３】


スタート
コンテンツ鍵Kで暗号化されたMPEG映像をIEEE1394の同期チャネル#xから受信。送信ノードから送られてきた暗号化されたデータであることを認識。ただし、復号化等は行わずに、そのまま無線網の無線同期チャネル#yに送信
S8701
送信ノードに認証要求を送信(中継ノードのIEEE1394側認証フォーマットBcertを含む)
S8702
送信ノードから認証要求を受信(送信ノードの認証フォーマットAcertを含む)
S8703
認証・鍵交換手続きを行い、認証鍵Kauth1を送信ノードと共有する
S8704
無線ノードから認証要求を受信(無線ノードの認証フォーマットDcertを含む)
S8705
無線ノードに認証要求を送信(中継ノードの無線網側の認証フォーマットCcertを含む)
S8706
認証・鍵交換手続きを行い、認証鍵Kauth2を無線ノードと共有する
S8707
R26へ

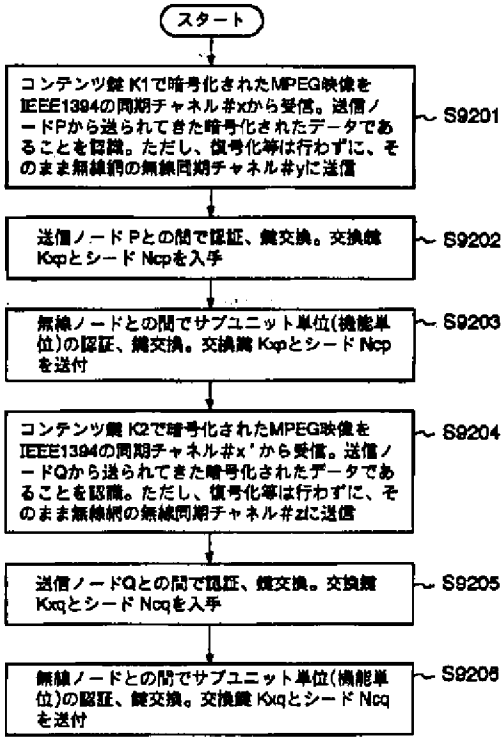
【図８５】


スタート
コンテンツ鍵Kで暗号化されたMPEG映像を無線同期チャネル#yから受信。中継ノードから送られてきた暗号化されたデータであることを認識
S8801
中継ノードに認証要求を送信(無線ノードの認証フォーマットDcertを含む)
S8802
中継ノードから認証要求を受信(中継ノードの認証フォーマットCcertを含む)
S8803
認証・鍵交換手続きを行い、認証鍵Kauth2を中継ノードと共有する
S8804
中継ノードから交換鍵Kxを受信(関数f(Kx, Kauth2)の形で)
S8805
交換鍵Kxを抽出
S8806
R27へ

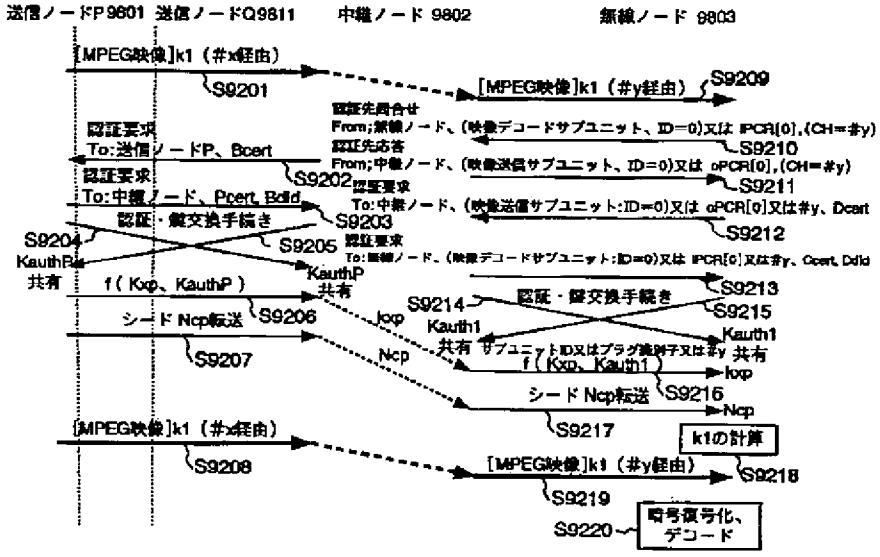
【図86】


R27
中継ノードからシードNcpを受信
S8807
コンテンツ鍵Kの計算
S8808
コンテンツ鍵Kで暗号化されたMPEG映像を無線同期チャネル#yから受信
S8809
コンテンツ鍵Kを使って暗号復号化、およびデコード
S8810

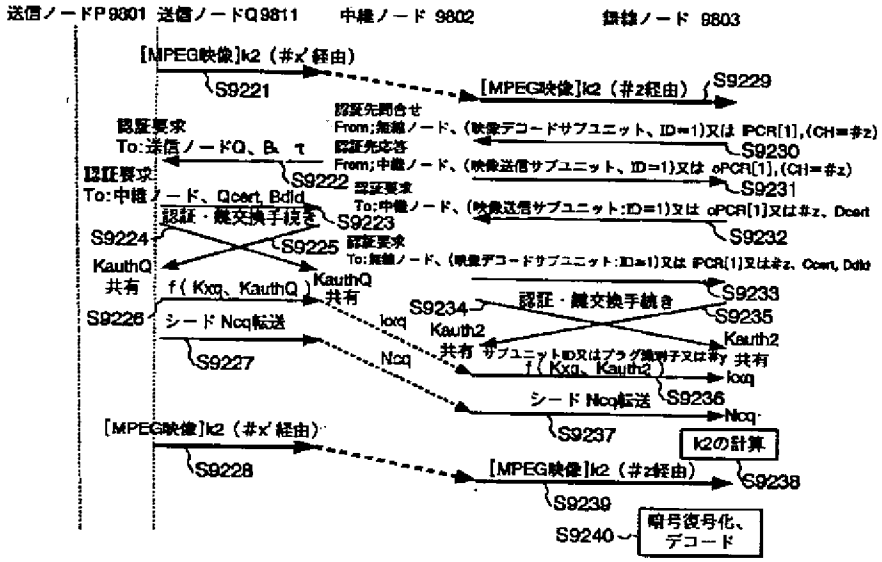
【図88】


スタート
コンテンツ鍵K1で暗号化されたMPEG映像をIEEE1394の同期チャネル#xから受信。送信ノードPから送られてきた暗号化されたデータであることを認識。ただし、復号化等は行わずに、そのまま無線網の無線同期チャネル#yに送信
S9201
送信ノードPとの間で認証、鍵交換。交換鍵Kxpとシード Ncpを入手
S9202
無線ノードとの間でサブユニット単位(機能単位)の認証、鍵交換。交換鍵 Kxpとシード Ncpを送付
S9203
コンテンツ鍵 K2で暗号化されたMPEG映像をIEEE1394の同期チャネル#x'から受信。送信ノードQから送られてきた暗号化されたデータであることを認識。ただし、復号化等は行わずに、そのまま無線網の無線同期チャネル#zに送信
S9204
送信ノードQとの間で認証、鍵交換。交換鍵Kxqとシード Ncqを入手
S9205
無線ノードとの間でサブユニット単位(機能単位)の認証、鍵交換。交換鍵 Kxqとシード Ncqを送付
S9206

【図89】


送信ノードP 9801
送信ノードQ 9811
中継ノード 9802
無線ノード 9803
[MPEG映像]k1（#x経由）
S9201
[MPEG映像]k1（#y経由）
S9209
認証先問合せ
From;無線ノード、(映像デコードサブユニット、ID=0)又は IPCR[0],(CH=#y)
認証先応答
S9210
認証要求
To:送信ノードP、Bcert
From;中継ノード、(映像送信サブユニット、ID=0)又は oPCR[0],(CH=#y)
S9202
認証要求
S9211
To:中継ノード、Pcert, Bdid
To:中継ノード、(映像送信サブユニット:ID=0)又は oPCR[0]又は#y、Dcert
認証・鍵交換手続き
S9203
S9212
S9204
S9205
認証要求
KauthP
共有
f(Kxp、KauthP)
S9213
S9214
認証・鍵交換手続き
S9215
シードNcp転送
S9206
Kxp
Kauth1
共有
Kauth1
共有
サブユニットID又はプラグ識別子又は#y
f(Kxp、Kauth1)
Kxp
S9207
Ncp
シードNcp転送
S9216
Ncp
S9217
[MPEG映像]k1（#x経由）
k1の計算
S9208
[MPEG映像]k1（#y経由）
S9218
S9219
暗号復号化、デコード
S9220

【図90】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
H04L 29/06		H04L 13/00	305Z	